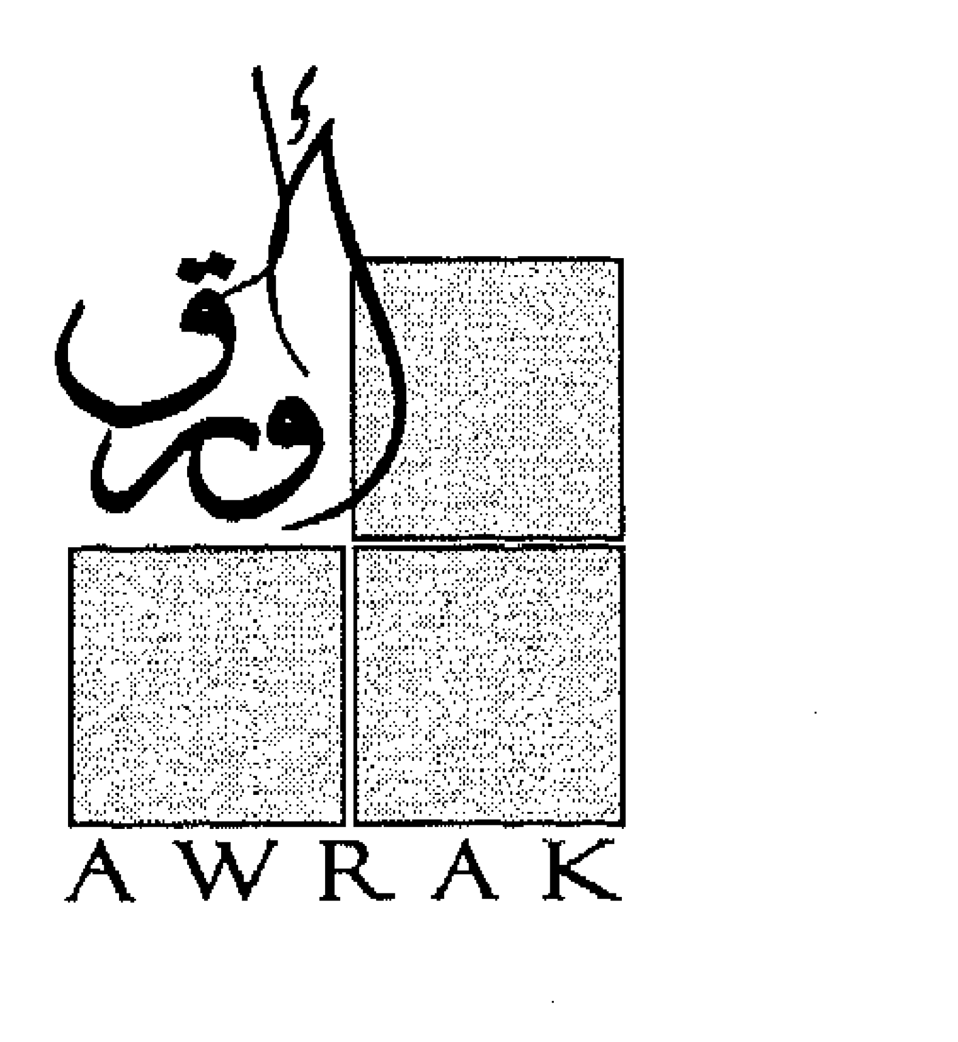


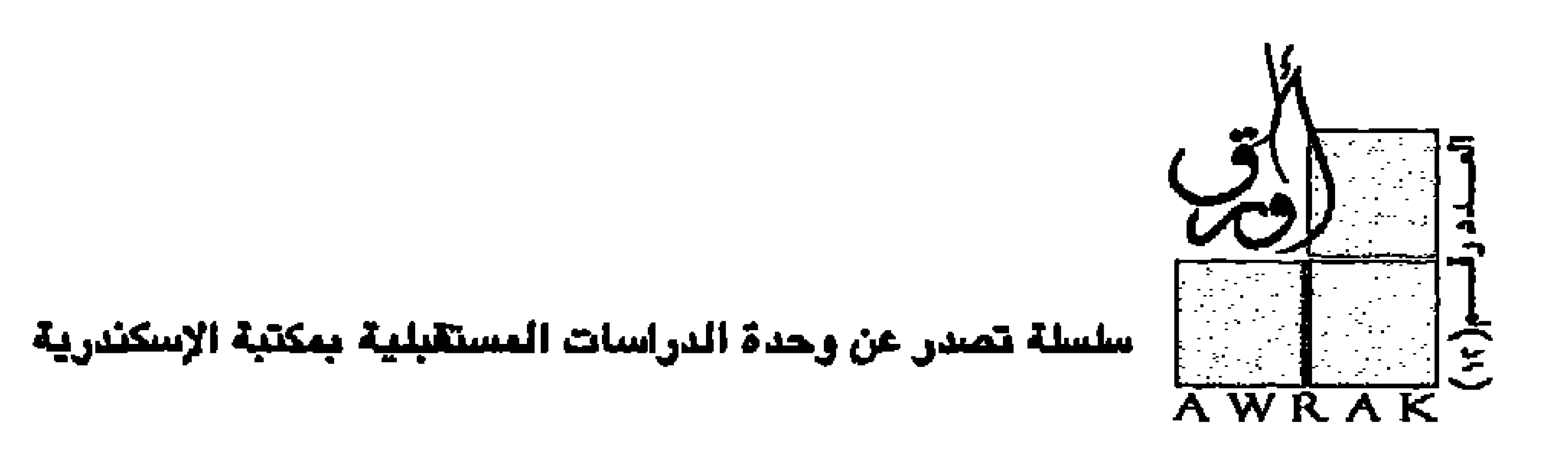

# القوة الإلكترونية وأبعاد التحول في خصائص القوة


تأليف: إيهاب خليفة



سلسلة تصدر عن وحدة الدراسات المستقبلية بمكتبة الإسكندرية


أوراق
AWRAK


أوراق
AWRAK
سلسلة تصدر عن وحدة الدراسات المستقبلية بمكتبة الإسكندرية



---

# القوة الإلكترونية وأبعاد التحول في خصائص القوة

تأليف: إيهاب خليفة

مكتبة الإسكندرية بيانات الفهرسة- أثناء النشر (فان)

خليفة، إيهاب.

القوة الإلكترونية و أبعاد التحول في خصائص القوة / إيهاب خليفة. - الإسكندرية، مصر : مكتبة الإسكندرية، وحدة الدراسات المستقبلية، 2014.

ص. سم. (أوراق ؛ 12)

تدمك 978-977-452-283-5

يشتمل على إرجاعات ببليوجرافية.

١. الفضاء الإلكتروني. ٢. الإنترنت. أ. مكتبة الإسكندرية. وحدة الدراسات المستقبلية. ب. العنوان. ج. السلسلة.

ديوي - 004.678　　　2014721265

ISBN:978-977-452-283-5

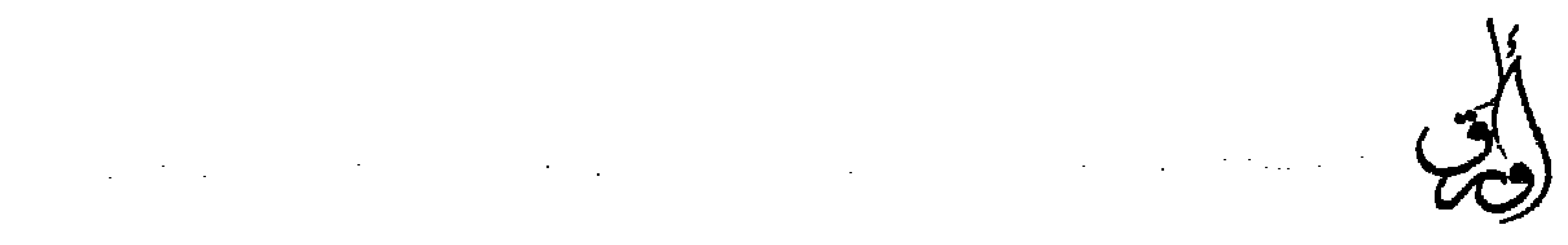
رقم الإيداع: 2014/10196

# المحتويات

## مقدمة

عرفت الإنسانية في صراعها نحو البقاء بيئات طبيعية سعت لاستكشافها واستغلالها وفرض نفوذها عليها، وهي **الأرض أو الإقليم البري**. ومع التوسع في الإقليم البري استطاع الإنسان أن ينطلق إلى بيئة أخرى، وهي **البحر أو الإقليم البحري**. ومع تطور التكنولوجيا الحديثة والتطور من المشي إلى السيارات والدبابات، ومن المراكب الشراعية إلى السفن البخارية ثم الغواصات النووية، أصبح للتكنولوجيا دور هام في حسم المعارك الحربية، فظهرت أهمية القوة البحرية إلى جانب القوة البرية. ومع التطور التكنولوجي أمكن القفز لبيئة طبيعية أخرى، وهي **الجو أو الإقليم الجوي**، وبدأت تحلق فيه الطائرات وظهرت أهميتها في تدمير مواقع العدو والتمهيد للمعارك الحربية. ومع التطور التكنولوجي المذهل في عالم الطيران والصواريخ أمكن استغلال بيئة طبيعية جديدة، وهي **الفضاء الخارجي**؛ من خلال الأقمار الصناعية. وبرغم أن الفضاء الخارجي لم يتم استغلاله عسكريًّا أو تجاريًّا مثلما تم استغلال البيئات الثلاثة السابقة، فإنه يشكل محورًا هامًّا في ربط هذه البيئات بعضها ببعض؛ حيث تتزايد أهميته في عالم الاتصالات والمعلومات.

وبفضل ثورة المعلومات، ومع ظهور الإنترنت ومواقع الويب ظهرت لدينا بيئة أخرى وهي **الفضاء الإلكتروني**، وبرغم أنها تختلف عن البيئات الأربعة الطبيعية



السابقة في كونها بيئة من صنع الإنسان Manmade، فإنها تتمتع بخصائص تشترك فيها مع تلك البيئات السابقة، وأصبح الفضاء الإلكتروني أحد العناصر الرئيسية التي تؤثر في النظام الدولي بما يحمل من أدوات تكنولوجية تلعب دورًا هامًا في عملية التعبئة والحشد في العالم، فضلاً عن التأثير فى القيم السياسية؛ فسهولة استخدامها ورخص تكلفتها ساعدا على قيامها بأدوار مختلفة في الحياة البشرية، سواء تجارية أو اقتصادية أو معلوماتية أو سياسية أو عسكرية أو أيديولوجية، هذا فضلاً عن أنها لم تعُد حكرًا على الدول فقط، وقد أصبح جليًا أن من يمتلك آليات توظيف هذه البيئة الإلكترونية الجديدة يصبح الأكثر قدرة على تحقيق أهدافه والتأثير في سلوك الفاعلين المستخدمين لهذه البيئة[١].

فالدولة عادةً ما تترجم قدراتها على تحقيق أهدافها الخارجية من خلال استخدامها لوسائل مختلفة؛ أهمها: الدبلوماسية، والقوة العسكرية، والدعاية، والأدوات الاقتصادية. ولكن أصبح من الأمور المستقرة في العلاقات الدولية أن مصادر قوة الدولة وأشكالها تتغير؛ فإلى جانب القوة الصلبة والتي تتمثل في القدرات العسكرية والاقتصادية، تزايد الاهتمام بالأبعاد غير المادية للقوة، ومن ثم برز دور القوة الناعمة التي تعتمد على جاذبية النموذج والإقناع. ومع ثورة المعلومات والقدرة على إنتاج التكنولوجيا المتطورة عن طريق الاختراع والإبداع، ظهر لدينا شكل جديد من أشكال القوة هو القوة الإلكترونية، وأصبح لديها تأثير على المستوى الدولي والمحلي؛ فمن ناحية أدت إلى توزيع وانتشار

---

(١) إيهاب عبد الحميد خليفة، «الفضاء الإلكتروني وتهديد الأمن القومي المصري»، المركز العربي لأبحاث الفضاء الإلكتروني، http://www.accronline.com/print_article.aspx?id=15383



القوة بين عدد أكبر من الفاعلين مما جعل قدرة الدولة على السيطرة على هذا الميدان موضع شك، مقارنة بالمجالات الأخرى للقوة، ومن ناحية أخرى جعلت القوة الإلكترونية بعض الفاعلين الأصغر في السياسة الدولية لديهم قدرة أكبر على ممارسة كلٍّ من القوة الصلبة والقوة الناعمة عبر الفضاء الإلكتروني، وهو ما يعني تغيرًا في علاقات القوى في السياسة الدولية(٢).

ويمكن التمييز بين مستويين للتغير الذي طرأ على مفهوم القوة؛ مستوى خاص بالعناصر المكونة للقوة، والأشكال المختلفة التي تتخذها القوة، ومستوى آخر خاص بالطرف الذي يمتلك القوة، خاصة مع امتلاك فاعلين من غير الدولة بعض مصادر القوة والتأثير في العلاقات الدولية. ومن ثم تسعى هذه الدراسة للوقوف على التغييرات التي أثرت في أشكال القوة، ولما للتكنولوجيا الحديثة من أثر هام في تطور ممارسة القوة والنفوذ في العلاقات الدولية، ولما للمعلومة من أثر هام في حسم الصراعات الدولية – كانت جديرة بالملاحظة معرفة أثر التكنولوجيا الحديثة والفضاء الإلكتروني في مفهوم القوة وخصائصها وتحولاتها. كما أنه من الضروري الوقوف على الفواعل والأطراف التي تمارس هذه القوة، سواء كانت فواعل من الدول أو من غير الدول. وفي هذه الحالة يصبح مجال ممارسة القوة هو الفضاء الإلكتروني، وأطرافه هي الدول والفواعل من غير الدول، وأدواته برامج حاسوب وفيروسات إلكترونية.

---

(٢) سعاد محمود أبو ليلة، «دورة القوة: ديناميكيات الانتقال من "الصلبة" إلى "الناعمة" إلى "الافتراضية"»، مجلة السياسة الدولية، ملحق اتجاهات نظرية القوة: كيف يمكن فهم تحولات القوة في السياسة الدولية؟ العدد ١٨٨ (٢٠١٢): ١٦.

## المبحث الأول

## الفضاء الإلكتروني وتحولات القوة

### القوة .. جدل قديم متجدد

تعد القوة من المفاهيم المعقدة، فرغم بساطتها الظاهرية من حيث كونها كلمة تتألف من خمسة أحرف، فإنه من الصعوبة تحديد ما المقصود بالقوة فعلاً. والجدل حول معنى القوة قديم متجدد؛ حيث جادل الفيلسوف الفرنسي ميشيل فوكو بأن أساس القوة هو التفاعل. ومن مقولاته الشهيرة: «إذا كان يفترض في القوة أنها توجد في الكون بطريقة مركزة أو منتشرة، فإنها لا توجد على هذا النحو، القوة توجد عندما تُستخدم»[٣]، في حين جادل ألفن توفلر بأن «المعرفة هي القوة، وأن امتلاك المعرفة هو الأساس لامتلاك الثروة والقوة العسكرية»[٤].

وإن تعددت واختلفت تعريفات القوة، فهي إجمالاً يمكن النظر إليها على أنها القدرة على التأثير في الآخرين للحصول منهم على نتائج محددة، يسعى الطرف الذي يقوم بعملية التأثير للحصول عليها. كما ربط «هانز مورجنثاو» القوة بفكرة التأثير أو التحكم في المكاسب، وعرّف القوة بأنها «القدرة على التأثير في سلوك

(٣) عبد العزيز العيادي، ميشيل فوكو.. المعرفة والسلطة (د.م: المؤسسة الجامعية للدراسات والنشر والتوزيع، ١٩٩٤): ٤٤.
(٤) ألفن توفلر، تحول السلطة، ترجمة لبنى الريدي (د.م: الهيئة المصرية العامة للكتاب، ١٩٩٥): ٢٥.



الآخرين»[٥]. وقد استفاد عالم الاجتماع «روبرت دال» من أفكار مورجنثاو حول القوة وقدم تعريفًا أكثر وضوحًا للقوة؛ حيث عرفها بأنها «القدرة على جعل الآخرين يقومون بأشياء متناقضة مع أولوياتهم، ما كانوا ليقوموا بها لولا ممارسة تلك القدرة»[٦]؛ حيث جادل ستيفن لوكس عام ١٩٧٤ في كتابه «القوة: رؤية راديكالية»؛ بأن «القوة مرتبطة بتحديد الأجندة، للتأثير في سلوك الدول، ومِنْ ثَمَّ لا تعني القوة بالضرورة الإكراه»[٧].

وهناك اتجاه آخر لتعريف القوة، عبر عنه كينيث والتز، حيث وسع مفهوم القوة ليشمل عناصر أخرى غير عسكرية، وحاول الربط بين قوة الدولة، وامتلاك عناصر؛ مثل المساحة، والموقع الجغرافي، والموارد المادية والطبيعية، والسكان، ودرجة النمو الاقتصادي، والتطور العسكري، والاستقرار السياسي والكفاءة[٨]. وقد طور جوزيف ناي أفكار لوكس، وقدم مفهومًا، ربما يكون أكثر تعقيدًا للقوة؛ حيث اهتم بعناصر القوة غير المادية؛ مثل الثقافة والقيم، من خلال مفهوم القوة الناعمة. وعرفها بأنها «قدرة الدولة على الحصول على ما تريده بالاعتماد على الجاذبية بدلاً من الإكراه[٩]». وتعبر القوة الناعمة عن الوجه الثاني للقوة؛ حيث تتمكن دولة ما من الحصول على النتائج التي تريدها؛ لأن الدول الأخرى معجبة بنموذجها، وتحاول أن تتبعه، وليس لأنه يتم إكراهها على ذلك. ومع ثورة المعلومات، أُضيف عنصر جديد لقوة الدولة؛ حيث أصبح من عناصر قوة الدولة

---

(٥) Hans J. Morgenthall, **Politics Among Nations** (New York: Alfred A. Knopf, 1948): 140.

(٦) Joseph S. Nye, **Cyber Power** (Cambridge: Harvard Kennedy School. Belfer Center for Science and International Affairs, 2010): 2.

(٧) Steven Lukes, **Power: A Radical View** (n.p.: British Sociological Association, 1974): 14.

(٨) Kenneth N. Waltz, **Man, the State and War: A Theoretical Analysis** (New York : Colombia University Press,1959): 159-160.

(٩) Joseph S. Nye, **Soft Power: The Means To Success In World Politics** (New York: Public Affairs, 2004): 2.

امتلاك التكنولوجيا والمعلومات، والقدرة على إنتاج التكنولوجيا المتطورة عن طريق الاختراع، والإبداع، ونشر الإبداع أيضًا(١٠).

ومن الأمور المستقرة في العلاقات الدولية أن مصادر قوة الدولة ومكونات نفوذها تتغير، وأن القوة العسكرية وحدها لم تعد تحقق الأهداف المرجوة التي تسعى الدولة لتحقيقها، وأن أشكال القوة متغيرة؛ فمنها القوة الصلبة، والتي تتمثل في القدرات العسكرية والاقتصادية، وهناك القوة الناعمة، والتي تتمثل في العوامل غير المادية كالثقافة والقيم(١١). ومع ثورة المعلومات تم إضافة عنصر جديد لقوة الدولة وهو القوة الإلكترونية؛ حيث أصبح من عناصر قوة الدولة امتلاك التكنولوجيا والمعلومات، والقدرة على إنتاج التكنولوجيا المتطورة عن طريق الاختراع والإبداع ونشر الإبداع أيضًا.

وإذا كانت الحرب هي الشكل التقليدي لاستخدام القوة، فإن شن الحرب لم يعد يقتصر على استخدام القوة العسكرية فقط، فكما رأى اثنان من جنرالات الحرب الصينيين ليانج وإكسيانج سو في كتابهما «حرب غير مقيدة»، فإن أدوات القوة سوف تُستخدم في الحروب، وكل المعلومات ستكون منتشرة في كل مكان، وستكون أرض المعركة في كل مكان. ومن ثم أصبحت القوة تعني كل شيء تقريبًا يسمح بممارسة الضغط النفسي والسياسي، الذي هو جوهر القوة من أجل تحقيق غايات محددة(١٢).

---

(١٠) ريهام مقبل، «مركب القوة: عناصر وأشكال القوة في العلاقات الدولية»، مجلة السياسة الدولية، ملحق اتجاهات نظرية القوة: كيف يمكن فهم تحولات القوة في السياسة الدولية؟ العدد ١٨٨ (إبريل ٢٠١٢): ٦-١٠.

(١١) **Nye, Soft Power: The Means To Success In World Politics.**

(١٢) إيمان رجب، «لماذا القوة؟» مجلة السياسة الدولية، ملحق اتجاهات نظرية القوة: كيف يمكن فهم تحولات القوة في السياسة الدولية؟ العدد ١٨٨ (إبريل ٢٠١٢): ٣.



ويعتبر مفهوم القوة من المفاهيم المركزية في فكر المدرسة الواقعية التي ترى أن السياسة الدولية هي عبارة عن صراع ونزاع من أجل القوة، وأن النظام الدولي يتسم بالفوضوية، ومن ثم تعتمد فيه الدول القومية على قدراتها، فالعالم هو عالم الصراع والحرب وهما أساس العلاقات الدولية، ولكل دولة مجموعة من المصالح التي تسعى إلى تحقيقها، وهي ثلاث مصالح رئيسية؛ مصلحة البقاء، ومصلحة تعظيم القوة العسكرية، ومصلحة تعظيم القوة الاقتصادية. وجميع تلك المصالح متشابكة؛ كل مصلحة مع الأخرى[١٣].

ومن ناحية أخرى أعادت النظرية الليبرالية تعريف القوة؛ حيث ترى أن القوة تتمثل ليس فقط في القوة العسكرية، ولكن أيضًا في القوة الاقتصادية. ويرى جوزيف ناي أن هذين النوعين يمثلان القوة الصلبة، ولكن هناك بعد آخر من القوة يمكن للدولة من خلاله تحقيق أهدافها؛ يتمثل في جاذبية النموذج والقيم والقدرة على الإقناع؛ إذ بإمكان دولة ما أن تنال النتائج التي تسعى لتحقيقها؛ وذلك لأن الدول الأخرى تريد أن تتبعها وتعجب بقيمها وتتشبه بها وتطمح للوصول إلى مستواها، وهو ما أطلق عليه ناي اسم القوة الناعمة[١٤].

وقد ارتبط الحديث عن القوة الناعمة كأحد أشكال القوة بمحاولات جوزيف ناي معالجة التحليل الضيق لمفهوم القوة الذي قدمته المدرسة الواقعية والذي كان يركز على القوة العسكرية؛ حيث ميز ناي بين ثلاثة أنماط من القوة الناعمة؛ هي: النمط الأول هو **الجاذبية Attraction**، ويشير إلى جذب الانتباه إما

---

(١٣) James E. Dougherty and Robert L. Pfaltzgraff, **Contending Theories of International Relations** (n.p.: Longman, 2001): 63–100.

(١٤) Ibid: 416–447.

بطريقة سلبية وإما إيجابية، والنمط الثاني هو **الإقناع Persuasion**، ويستخدم للتأثير في معتقدات الآخرين وردود أفعالهم دون التهديد باللجوء إلى القوة، وينصرف النمط الثالث إلى وضع جدول الأعمال أو ما يطلق عليه **Agenda Setting** وتحديد أولويات الدول الأخرى بما يخدم أو يتفق مع أولويات الدولة التي تمارس القوة الناعمة(١٥).

## أثر التكنولوجيا في تحولات القوة

### ١- تغير أشكال القوة بين الصلبة والناعمة

كان من السهل قديمًا تقييم قدرات وإمكانيات الدول، وقياس قوتها؛ حيث ارتبط تعريف القوة تاريخيًّا بـ«القوة في الحرب»، واعتبرت عناصر مثل السكان، والأرض، والموارد الطبيعية، والقوة الاقتصادية، والاستقرار السياسي، والقوة العسكرية، هي المكونات الرئيسة لمفهوم القوة، فإذا كان لدى الدولة أسطول قوي وجيش مدرب بشكل جيد، وكذلك قوة ديموغرافية واقتصادية، فمن المحتمل أن تكون قادرة على إجبار أو إكراه، أو حتى رشوة جيرانها، ومن ثم دفعهم إلى الامتثال لأهدافها.

لكن عبر القرون، وازدهار التكنولوجيا وتطورها، تغيرت مصادر القوة، فلم تعد تلك المصادر التقليدية التي تميزت بها القوى الدولية التقليدية في قرون ماضية، فعلى سبيل المثال كان عنصر السكان أحد مصادر القوة؛ وذلك من خلال دفع الضرائب التي تستخدم في التمويل العسكري وتجنيد المواطنين الصالحين في الجيش، وكان عنصرًا حاسمًا في المعارك الحربية، بينما نجد حاليًّا أن امتلاك

(١٥) مقبل، «مركب القوة: عناصر وأشكال القوة في العلاقات الدولية»: ٧.

التكنولوجيا العسكرية الحديثة والأسلحة غير التقليدية، أصبحت عناصر حاسمة في المعارك الحربية.

وقد ساهم العلم والتكنولوجيا في تغيير موازين القوى خلال العصور المختلفة، فانتقلت القوة من إسبانيا والبرتغال القوتين العظميين في أوروبا في القرن الخامس عشر الميلادي، إلى هولندا التي أصبحت القوى العظمى في القرن السابع عشر، واحتلت المرتبة الأولى من حيث قوتها البحرية الضاربة. ولكن اندلاع الحروب بين هولندا وبين إنجلترا وفرنسا أضعف من قوة هولندا، وأصبحت بريطانيا وفرنسا من أقوى الدول الأوروبية. وفي منتصف القرن العشرين تغير الميزان الدولي من فرنسا وبريطانيا، إلى الولايات المتحدة الأمريكية والاتحاد السوفيتي، وذلك عقب امتلاك الأسلحة النووية، وتطوير صواريخ عابرة للقارات، وبذلك ساهم العلم والتكنولوجيا في تغيير موازين القوى الدولية، وانتقالها من دول إلى أخرى ومن إقليم إلى آخر.

ويشير جوزيف ناي إلى أن بَعْضَهم يفكر في القوة بصورة خاطئة، ويرى أن تعريف القوة بأنها القدرة على جعل الآخرين يفعلون ما لا يريدون، هو في ظاهره قد يكون غير دقيق، خاصة إذا كان الأمر يتعلق بتغيير سلوكيات الآخرين. ويجادل بأنه يجب معرفة أولويات الآخرين؛ حتى نستطيع قياس التغير في السلوك نتيجة القوة. ويدلل على ذلك بأن الديكتاتور الذي يسعى لإعدام معارض سياسي بريء قد يفقد معنى قوته إذا كان ذلك البريء يسعى بالفعل للاستشهاد، كما أنه مخطئ من يظن أن صياح الديك هو الذي يجعل الشمس تشرق[١٦].

---

(١٦) Nye, Soft Power: The Means To Success In World Politics: 2.

فالقوة الصلبة بهذه الصورة تعني القوة المشتركة السياسية والاقتصادية والعسكرية؛ أي القوة في صورتها الخشنة التي تعني الحرب، والتي تستخدم فيها الجيوش. وهذه القوة تعني الدخول في مزالق خطرة، ونتائجها تكون في منتهى الخطورة على الدولة نفسها، كما حدث مثلاً في الحرب العالمية الثانية مع اليابان وألمانيا النازية.

ويؤكد ناي أنه يمكن الحصول على النتائج المرجوة والتأثير في سلوكيات الفاعلين دون اللجوء إلى القوة، وهو ما يدفع بَعْضَهُمْ إلى تنفيذ أوامر البابا، ليس خوفًا من عقاب، ولكن إيمانًا بسلطته الأخلاقية والروحية، وبنفس المنطق نجد أن هناك مؤيدين لزعيم القاعدة – السابق – أسامة بن لادن من المسلمين المتشددين، ليس خوفًا من عقاب أو تهديدات، ولكن إيمانًا بشرعية أهدافه(١٧).

وقد عرف جوزيف ناي في تسعينيات القرن المنصرم مفهوم القوة الناعمة بأنه القدرة على جذب الآخرين والتأثير فيهم من خلال القيم والمعتقدات، وليس من خلال التهديد أو استعمال القوة العسكرية أو الاقتصادية(١٨)، أي القدرة على الحصول على النتائج المرجوة من خلال الجاذبية وليس الإكراه، وذلك بالاعتماد على جاذبية ثقافة الدولة، وأفكارها السياسية، وسياساتها(١٩).

ومن ثم تشكل القوة الناعمة أحد أشكال القوة التي تستخدمها الدول في سياستها الخارجية، وتشكل إطارًا عامًّا من الأنماط والسلوكيات الثقافية التي تسعى من خلالها الدول لنشرها على المستوى الخارجي من أجل تحقيق

(١٧) Ibid.

(١٨) Joseph S. Nye, The Decline of America's Soft Power (n.p.: Foreign Affairs, 2004).

(١٩) Nye, Soft Power: The Means To Success In World Politics.

أهدافها؛ وذلك عبر مجتمع المعلومات؛ مثل: نشر الأفكار والمعلومات، ودعم قنوات البث الإذاعي والإرسال التليفزيوني، وترويج سلع ثقافية وخدمات وبرامج معلوماتية، يكون هدفها دعم المعارضة للنظم القائمة[٢٠]، أو السياسات الخاصة بالمنظمات الدولية، وتقديم المعونات الاقتصادية، وتنفيذ مشروعات اقتصادية وتجارية، أي باختصار تحقيق هدف تم الاتفاق عليه وعلى إنجازه بأساليب فكرية وإقناعية دون اللجوء للعنف.

ويأتي في سياق القوة الناعمة دور الإعـلام في عصر العولمة أو «إعلام العولمة» والذي يعني تعاظم قدرة وسائل الإعلام والمعلومات على تجاوز الحدود السياسية والثقافية بين الدول والمجتمعات بفضل وسائل التكنولوجيا الحديثة[٢١]؛ حيث أصبح امتلاك القدرة على المساهمة في الثورة المعلوماتية أساس القوة في العلاقات الدولية، والوسيلة التي تتمكن خلالها دولة أو بعض الدول من بسط نفوذها والهيمنة على الدول الأخرى في النظام الدولي الجديد؛ حيث تطور مفهوم القوة من القوة العسكرية ثم القوة الاقتصادية إلى قوة المعلومات ومدى قدرة الذكاء والنشاط البشري على توظيفها واستخدامها[٢٢].

وحسب ناي، فإن هناك خمسة تحولات دولية ساهمت في تراجع دور القوة الصلبة أو على الأقل قلّلت من فاعليتها، تمثلت في الاعتماد الاقتصادي المتبادل بين الدول بما ساهم في الحد من الاستخدام الصلب للقوة لمخاطرها

---

(٢٠) يحيى اليحياوي، «عن قوة أمريكا الناعمة»، تكنولوجيا: عولمة، إعلام، ثقافة، http://www.elyahyaoui.org

(٢١) أدهم عدنان طبيل، «الإعلام الحديث في ظل العولمة»، دنيا الرأي، http://pulpit.alwatanvoice.com/articles/2007/05/25/89911.html

(٢٢) إسراء أحمد، وشريف رشدي، الواقع الافتراضي والتغيير السياسي في العالم: دراسة في ثورات الوطن العربي (د.م: مركز المعلومات ودعم اتخاذ القرار، ٢٠١١): ٤٣.



على النمو الاقتصادي، فضلاً عن ظهور فواعل أخرى غير الدول أصبحت قادرة على ممارسة أنواع القوة؛ مثل الفاعلين غير القوميين، وكذلك الشركات متعددة الجنسية، والمنظمات الدولية سواء الحكومية أو غير الحكومية، والجماعات الإرهابية، بالإضافة إلى انبعاث النزعات القومية وهو ما صعّب عملية استخدام القوة، فعلى سبيل المثال، كانت بعض المواقع العسكرية الصغيرة قادرة على إدارة إمبراطورية مثل الإمبراطورية البريطانية. لكن في الوقت الحاضر، فإن الولايات المتحدة، على سبيل المثال، وجدت أنه من الصعب إخضاع العشائر الصومالية أو تهدئة الوضع في العراق،حتى مع زيادة عدد قواتها. وكذلك ساهم انتشار التكنولوجيا، خاصة في مجال تطوير الأسلحة النووية، في تعادل قوة الأطراف في أرض المعركة. وأخيرًا التغير الحادث في القضايا السياسية وظهور قضايا تعجز القوة الصلبة عن حلها؛ مثل الفقر والتلوث وانتشار الأوبئة والجريمة المنظمة والتغيرات المناخية. كما أن استخدام القوة العسكرية أصبح مكلفًا جدًا مقارنة بما كان في القرون الماضية(٢٣).

فحينما تبدو السياسة الأمريكية مقبولة ومشروعة في أعين الآخرين، على ما يقول ناي، «يتعاظم دور القوة الناعمة أكثر، وبموازاة ذلك، تتراجع الحاجة إلى استخدام القوة التقليدية. وعلى العكس من ذلك، فكلما تضخم استخدام القوة الإكراهية، وضعفت شرعية مثل هذا الاستخدام، يتضاءل معها النفوذ الثقافي والسياسي والتجاري، وكل ما يدخل ضمن دائرة القوة الناعمة(٢٤)».

---

(٢٣) «القوة الناعمة الأمريكية آفاقها وتحدياتها»، الصحوة للدراسات (١٣ نوفمبر ٢٠١٢)، http://www.essahwa.com/?p=131

(٢٤) رفيق عبد السلام، الولايات المتحدة الأمريكية بين القوة الصلبة والقوة الناعمة (الدوحة: مركز الجزيرة للدراسات، ٢٠٠٨): ٨٨.

ومن ثم، فإذا كانت القوة الصلبة تنبع أساسًا من القدرات العسكرية والاقتصادية، فإن القوة الناعمة تتأتى من جاذبية النموذج، وما يمتلكه من قدرة التأثير والإغراء للنخب والجمهور على السواء. فالقوة الناعمة كما يرى ناي هي قوة جذب، وتتضح في تعدد الوسائل التي يمكن اللجوء إليها للحصول على النتائج المرجوة دون اللجوء إلى استخدام العصا أو الجزرة.

يؤكد ناي في كتابه القوة الناعمة أن مصادر هذه القوة الناعمة لدى الدول ثلاثة مصادر؛ هي:

- الثقافة: والتي تكمن في جاذبيتها للآخرين.
- القيم السياسية: والتي تترسخ في النخبة الحاكمة والمحكومة.
- السياسة الخارجية: والتي ينظر إليها مختلف الفواعل الدولية على أنها شرعية وأخلاقية.

ويرى ناي أن الثقافة هي نسق من القيم والممارسات التي تخلق معنى للمجتمع، فإذا تبنت الدولة في سياساتها ثقافات وقيمًا عالمية يشارك الآخرون فيها وليست قيمًا ضيقة تعبر عن ثقافة خاصة، فإن من شأن ذلك حصول هذه الدولة على النتائج التي ترجوها. كما أن القيم التي تعتقد فيها الدولة كالديمقراطية، والسياسات التي تتبعها كحقوق الإنسان، تضفي مزيدًا من الشرعية على أهداف الدولة بما يساعد على تحقيقها[٢٥].

ولكن هذا لا يعني إغفال دور القوة الصلبة، فكلتاهما وجهان لعملة واحدة، ولا تغني إحداهما عن الأخرى، فكلتاهما تؤثر في السلوك وتسعى لدفع الآخرين

---

(٢٥) Nye, Soft Power: The Means To Success In World Politics: 10–14.



للقيام بأفعال لم يكونوا يقومون بها. ولكن تختلف أدوات ممارسة هاتين القوتين، فبينما تعتمد القوة الأولى على الإكراه تعتمد القوة الثانية على الجاذبية، وتختلفان أيضًا في مصادرهما، فبينما تعتمد الأولى على القوة العسكرية والاقتصادية، تعتمد الثانية على القيم والثقافات والمؤسسات(٢٦).

**٢- الفضاء الإلكتروني وتحولات القوة (القوة الإلكترونية)**

بفضل ثورة المعلومات، ومع ظهور الإنترنت ومواقع الويب أصبح الفضاء الإلكتروني أحد العناصر الرئيسية التي تؤثر في النظام الدولي بما يحمل من أدوات تكنولوجيا تلعب دورًا مهمًّا في عملية التعبئة والحشد في العالم، فضلاً عن التأثير فى القيم السياسية وأشكال القوة المختلفة، سواء كانت صلبة أو ناعمة.

وقد كان لظهور الفضاء الإلكتروني والشبكة العنكبوتية أثر هام في الحياة البشرية؛ فسهولة استخدامها ورخص تكلفتها ساعدا على قيامها بأدوار مختلفة في الحياة البشرية، سواء تجارية أو اقتصادية أو معلوماتية أو سياسية أو عسكرية أو أيديولوجية أو غيرها من المهام التي يمكن أن تقوم بها، فالذي يدير العالم الآن آحاد وأصفار غاية في الصغر. وقد أصبح جليًّا أن من يمتلك آليات توظيف هذه البيئة الإلكترونية الجديدة فإنه الأكثر قدرة على التأثير في سلوك الفاعلين المستخدمين لهذه البيئة.

ويعتبر الفضاء الإلكتروني بيئة مصنوعة وحديثة؛ حيث يستجيب للتغيرات بصورة سريعة أكبر من البيئات الطبيعية الأخرى؛ وذلك لاعتماده على التكنولوجيا الحديثة واستجابته السريعة للتطورات التكنولوجية، فإذا كان من الصعب

---

(٢٦) Ibid: 7–9.



السيطرة أو التحكم أو التنقل بين الإقليم البري أو البحري أو الجوي أو الفضاء الخارجي، فإنه يمكن التجول بلا حدود في الفضاء الإلكتروني بمجرد ضغطة على مفتاح التشغيل الخاص بالكمبيوتر، فهو يتميز بسهولة الاستخدام ورخص التكلفة وسهولة الحصول على المعلومات وتوافرها، فضلاً عن إمكانية التخفي وعدم الظهور بالشخصية الحقيقية الملموسة على أرض الواقع. وقد شجع كل ذلك على تعدد الفاعلين المستخدمين للفضاء الإلكتروني، فشمل بذلك أفرادًا وجماعات ودولًا ومنظمات دولية وشركات. كما تعددت استخداماته، فأصبح له استخدامات تجارية ومالية واقتصادية وعسكرية واجتماعية وعلمية ومعلوماتية. فإذا كان من الصعب تحريك أسطول دولة معينة في المحيط أو الإقليم البحري للقيام بمهمة معينة، فإنه من اليسير جدًّا إرسال جيش جرار من الفيروسات وبرامج الكمبيوتر التي تستطيع القيام بعمليات معلوماتية على قدر عالٍ من الأهمية.

وهناك ثلاثة عناصر أساسية أفرزتها ثورة المعلومات؛ هي: المعلومة Information، والفضاء الإلكتروني Cyberspace، والطابع الإلكتروني Digital. وتعتبر كلمة Cyber مقتبسة من علم Cybernetics؛ وهو عبارة عن نظرية الاتصالات والتحكم المنظم في التغذية المرتدة التي تعتمد عليها دراسات الاتصالات والتحكم في الحياة وفي الآليات التي صنعها الإنسان، أي علم دراسة الاتصال والتحكم الآلي في النظم العصبية للكائنات الحية ومحاكاة الآلات لها. وتستخدم كلمة Cyber مرتبطة بكلمة Space، لتعبر عن الفضاء الإلكتروني لتضم كل الاتصالات والشبكات وقواعد المعلومات والبيانات ومصادر المعلومات[٢٧].

ويختلف الفضاء الإلكتروني عن الغلاف الجوي أو الفضاء الخارجي في أن الفضاء الإلكتروني يعمل وفق قوانين فيزيائية مختلفة عن قوانين الفضاء الخارجي،

(٢٧) عادل عبد الصادق، الإرهاب الإلكتروني: القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة (القاهرة: مركز الأهرام للدراسات السياسية والاستراتيجية، ٢٠٠٩): ٣٠-٤٠.

فمثلاً لا تزن المعلومات شيئًا، ولا تمتلك كتلة مادية، وبإمكان المعلومات أن تظهر للوجود وتختفي منه، ويتم تعديل وتبادل المعلومات خلال نظم مرتبطة بالبنية التحتية، ويتطلب الفضاء الإلكتروني وجود هيكل مادي من أجهزة الكمبيوتر وخطوط الاتصالات، ومن ثم فإن ما يعمل داخل هذه الأجهزة يمثل نمطًا من القوة والسيطرة، وتصبح القيمة الحقيقة للفضاء الإلكتروني هي الاستفادة من كم المعلومات الموجودة داخله، والمساهمة في التحكم بها في إطار وشكل إلكتروني.

ويعد الفضاء الإلكتروني مجالاً عامًّا وسوقًا مفتوحة، ويدلل على وجود شبكة من التواصل والعلاقات بين من يستخدمونه ويتفاعلون معه مع انتقال كافة مجالات الحياة من إعلام وصحة وتعليم وحكومة ومواطنة واقتصاد وسياسة إلى الفضاء الإلكتروني فيما يشبه بالحياة الأخرى. وإلى جانب ذلك أصبح الفضاء الإلكتروني وسيطًا ووسيلة في نفس الوقت لشن الهجوم وتنفيذ الأعمال العدائية بين الخصوم كغيره من المجالات كالجو أو الفضاء أو البحر، فهو بمنزلة وسيط جديد للصراع. ويحوي الفضاء الإلكتروني كمًّا هائلاً ومتسعًا عبر الشبكات ونظم المعلومات والاتصالات تربطه مع الفضاء الخارجي والأقمار الصناعية. وعلى الرغم من درجة التشابه بينه وبين الفضاء الخارجي، فإنه يختلف في أن الفضاء الإلكتروني تم بناؤه من قبل الإنسان ولم يوجد في الطبيعة[٢٨].

وتستخدم الدول الفضاء الإلكتروني لاعتبارات الأمن والقوة العسكرية بشكل جعل عديدًا من الدول تدخل الفضاء الإلكتروني ضمن حساباتها

(٢٨) الصادق، الإرهاب الإلكتروني: ٣٥-٤٠.

الاستراتيجية وأمنها القومي، وهذا إلى جانب دور الفضاء الإلكتروني في تحقيق الرفاهية الاقتصادية والحصول على موارد الثورة والسلطة وتحقيق التفوق السياسي، وتعظيم معرفتها وسباقها العلمي والبحثي، والقدرة أيضًا على تحقيق السلم والأمن والتفاهم الدولي من خلال دور الفضاء الإلكتروني كأداة اتصال ووسيلة إعلام دولية.

وتتضح العلاقة ما بين الفضاء الإلكتروني والأمن الدولي؛ حيث يوجد المحتوى المعلوماتي العسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي في الفضاء الإلكتروني، خاصة مع التوسع في تبني الحكومات الإلكترونية من جانب العديد من الدول واتساع نطاق مستخدمي وسائل الاتصال وتكنولوجيا المعلومات في العالم؛ حيث تصبح قواعد البيانات القومية في حالة انكشاف خارجي، وهذا ما يعرضها لخطر التعرض لهجمات الفضاء الإلكتروني، إلى جانب الدعاية والمعلومات المضللة ونشر الشائعات أو الدعوة لأعمال تحريض أو دعم المعارضة الداخلية للنظام الحاكم.

ويعتبر الصراع الإلكتروني أحد أوجه الصراع الدولي؛ حيث يستطيع أحد أطراف الصراع أن يوقع خسائر فادحة بالطرف الآخر، وأن يتسبب في شل البنية المعلوماتية والاتصالاتية الخاصة به، وهو ما يسبب خسائر عسكرية واقتصادية فادحة، من خلال قطع أنظمة الاتصال بين الوحدات العسكرية بعضها وبعض، أو تضليل معلوماتها أو سرقة معلومات سرية عنها، أو من خلال التلاعب بالبيانات الاقتصادية والمالية وتزييفها أو مسحها من أجهزة الحواسيب، وبالرغم من



فداحة الخسائر، فإن الأسلحة بسيطة لا تتعدى الكيلو بايتس، تتمثل في فيروسات إلكترونية تخترق شبكة الحاسب الآلي وتنتشر بسرعة بين الأجهزة، وتبدأ عملها في سرية تامة وبكفاءة عالية، وهي في ذلك لا تفرق بين المقاتل والمدني، وبين العام والخاص، وبين السري والمعلوم[٢٩].

ولما للتكنولوجيا الحديثة من أثر في مفهوم القوة وتحولاتها، ظهر مفهوم القوة الإلكترونية Cyber Power؛ حيث يعرفها جوزيف ناي بأنها «القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء الإلكتروني، أي أنها القدرة على استخدام الفضاء الإلكتروني لخلق مزايا، والتأثير في الأحداث المتعلقة بالبيئات الواقعية الأخرى وذلك عبر أدوات إلكترونية»[٣٠]. ويعرفها دانيال كويل Daniel T. Kuehl بأنها «القدرة على استخدام الإنترنت لخلق مزايا، والتأثير في الأحداث في البيئات التشغيلية كافة من خلال أدوات القوة[٣١]».

يرى جوزيف ناي أن القوة الإلكترونية مرتبطة بامتلاك المعرفة التكنولوجية، والقدرة على استخدامها. وهي تعني القدرة على استخدام الفضاء الإلكتروني في خلق مميزات والتأثير في الأحداث التي تجري عبر البيئات التشغيلية Operational Environments، وعبر أشكال وأدوات القوة المختلفة، سواء كانت عسكرية أو اقتصادية أو دبلوماسية أو معلوماتية[٣٢]، وقد حدد ناي ثلاثة أنواع من الفاعلين

(٢٩) خليفة، «الفضاء الإلكتروني وتهديد الأمن القومي المصري».

(٣٠) Joseph S. Nye, **Cyber Power**: 4.

(٣١) Daniel T. Kuehl, "From Cyber Space to Cyber Power: Defining the Problems", in **Cyber Power and National Security**, edited by Franklin D. Kramer, Stuart Starr, and Larry K. Wentz (Washington, DC: National Defense University, 2009): 16.

(٣٢) Kuehl, "From Cyber Space to Cyber Power: Defining the Problems": 48.



الذين يمتلكون القوة الإلكترونية. يتمثل النوع الأول في الدولة، والنوع الثاني في الفاعلين من غير الدول، والنوع الثالث يتمثل في الأفراد. وقد حدد ناي أنماطًا لاستخدام موارد القوة الافتراضية، وميز بين الاستخدام الناعم لها والاستخدام الصلب.

ويجادل جوزيف ناي بأن مفهوم القوة الإلكترونية يشير إلى «مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الإلكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل[٣٣]».

وتتعدد أدوات ممارسة القوة في العلاقات الدولية وفقًا لقدرات وإمكانيات ورغبات القوى المشاركة فيه، فقد تكون القوة العسكرية هي إحدى أهم هذه الأدوات. وقد تكون القوة الاقتصادية والحصار الاقتصادي والمالي هو العامل الرئيسي للسيطرة على الخصم وممارسة القوة عليه، وقد تكون الأداة المعلوماتية من خلال وسائل الاتصال والتكنولوجيا الحديثة والإنترنت – هي العامل الرئيسي لحسم صراع بين دولتين.

إلا أن ممارسة القوة والنفوذ قد تطورت بشكل هائل نتيجة للتطور الكبير في المعلومات؛ مما جعل هذه المعلومات هي الهدف الأساسي الذي تسعى الدول للحصول عليه. هذه المعلومة هي التي مكنت الدول من إنتاج السلاح النووي، وظل هذا التطور مستمرًّا؛ حيث اعتمدت كل مرحلة من مراحل التطور الإنساني

---

(٣٣) **Joseph S. Nye, Cyber Power: 3.**

على سلطة أو قوة من طبيعة معينة تتناسب مع متطلبات هذه المرحلة. ولقد أثرت هذه السلطة أو القوة بصورة مباشرة أو غير مباشرة في أدوات الصراع بين المجتمعات وآلياتها، وأفرزت مفردات ومكونات تكاملت معًا لتنتج نظامًا دوليًا سيطرت مفاهيمه بعض الوقت أو كل الوقت. وفي هذا الإطار تميز عصرنا الحالي بظاهرة الثورة العلمية والتكنولوجية. ولقد أزاحت وحيّدت التكنولوجيا كثيرًا من عناصر القوة عن مواقعها التي تربعت عليها فترة طويلة. مما عرّض المفهوم التقليدي للقوة إلى انتقادات. وأُفصح عن محتوى جديد للقوة فلم يعد ما في يد الدولة من قدرات عسكرية أو ما تمتلكه من أموال وثروات، كافية لبلورة دورها كقوة مؤثرة وفاعلة[٣٤].

وأصبحت القوة الإلكترونية حقيقة أساسية في العالم بكل مظاهرها المتنوعة وبما عمل على دعم ومساندة العمليات الحربية والقوة الاقتصادية والسياسية ودور ثورة المعلومات والمعرفة في بروز مجتمع المعلومات الدولي والاقتصاد الإلكتروني الجديد الذي أثر في طبيعة النظام الدولي فيما يتعلق بالتقسيم الدولي للعمل، وهو الذي يحدد آفاق النمو أمام مختلف البلاد، ويعمل أيضًا على توزيع الموارد الاقتصادية ومستويات النمو الاقتصادي، وأنماط التفاعل بين القوى الاقتصادية الدولية، والتأثير في القوة السياسية بالتأثير في عمليات صنع القرار في النظام الدولي.

(٣٤) الصادق، الإرهاب الإلكتروني: ٥٠–٥٨.



ويتضمن مفهوم القوة الإلكترونية تغطية كافة القضايا التي تتعلق بالتفاعلات الدولية، والتي تشمل القضايا العسكرية والاقتصادية والسياسية والثقافية والإعلامية وغيرها، وتختلف عن مسمى الحرب الإلكترونية التي تقتصر على التطبيقات العسكرية للفضاء الإلكتروني، ويتم الإشارة إليه بالهجوم الإلكتروني.

وإذا كانت ثورة المعلومات لها تأثير في تطوير الجوانب العسكرية للدول، فإن لذلك أبعادًا سياسية واجتماعية؛ حيث ازدادت القدرات التدميرية للأسلحة. وهنا يثور تساؤل جدلي حول الدور الذي تلعبه التكنولوجيا في الحياة البشرية. فإذا كان لها مميزات تخدم الجنس البشري، فإن لها عيوبًا تفضي إلى القضاء عليه. ويثور تساؤل آخر حول دور التكنولوجيا في التأثير في القوميات الوطنية والثقافات الخاصة، والتي أصبحت عرضة للتأثير والتأثر؛ بفضل ثورة الاتصالات وتكنولوجيا المعلومات؛ حيث أصبحت السيطرة الثقافية لمن يمتلك التكنولوجيا ويستطيع أن يوظفها.

## المبحث الثاني

# انتشار القوة والفواعل الدولية في مجال استخدام القوة الإلكترونية

إن الثورة المعلوماتية قد أفرزت القوة الإلكترونية كشكل جديد من أشكال القوة. وهذه القوة لها تأثير في علاقات القوة على مستوى السياسة الدولية، فمن ناحية أدت إلى توزيع القوة بين عدد أكبر من الفاعلين مما جعل قدرة الدولة على السيطرة على هذا الميدان موضع شك، مقارنة بالمجالات الأخرى للقوة. ومن ناحية أخرى جعلت القوة الإلكترونية الفاعلين الأصغر في السياسة الدولية لديهم قدرة أكبر على ممارسة كلٍّ من القوة الصلبة والقوة الناعمة عبر الفضاء الإلكتروني، وهو ما يعني تغيرًا في علاقات القوى في السياسة الدولية[٣٥].

### المقصود بانتشار القوة

يعد جوزيف ناي أبرز المستخدمين لمفهوم انتشار القوة، ووفقًا له يرى أن هذه الظاهرة هي أكثر حداثة وغير مألوفة وتفرض تحديات جديدة على الدول، ويعرفها ناي بأنها: «تزايد القضايا ومجالات التأثير والتفاعل الواقعة خارج نطاق السيطرة الكلية للدولة، بما فيها الدول الأكثر قوة مع ظهور فاعلين جدد يتمتعون بصور جديدة من القوة»[٣٦]، أي أنها تعني مشاركة فواعل من غير الدول في موارد القوة التي كانت حكرًا على الفواعل من الدول.

---

(٣٥) منقول بتصرف، أبو ليلة، «دورة القوة: ديناميكيات الانتقال من "الصلبة" إلى "الناعمة" إلى "الافتراضية"»: ١٦.

(٣٦) Joseph S. Nye, Cyber Power: 113.



فإذا كان انتقال القوة ومراكز السيطرة الدولية من دولة إلى أخرى هو أمر مألوف في التفاعلات الدولية عبر العصور، ويمكن ملاحظته في ظهور مراكز دولية تزاحم الولايات المتحدة الأمريكية؛ مثل الصين والاتحاد الأوروبي، فإن انتشار القوة ظاهرة حديثة، ارتبطت بتعاظم دور الفاعلين من غير الدول؛ وذلك لأن المعلومة لم تعد حكرًا على الدول، فالقطاع الخاص يساهم بنسبة كبيرة في امتلاك وإدارة التكنولوجيا الحديثة ووسائل الاتصالات والمعلومات. ففي السبعينيات كان إمكانية الحصول على صورة للكرة الأرضية حكرًا على الولايات المتحدة الأمريكية والاتحاد السوفيتي، لما يمتلكان من تكنولوجيا تمكنهما من الحصول على ذلك. أما الآن ونتيجة للتقدم التكنولوجي فيمكن لأي فرد أن يحصل على صورة للكرة الأرضية وبأبعاد وفقًا لاحتياجاته من خلال برنامج Google Earth. وتراجعت سيادة الدولة لأول مرة منذ صلح وستيفليا ١٦٤٨ الذي أسس لنظام دولي قائم على سيادة الدول القومية، بل يجادل بعض الباحثين بأن ثورة المعلومات سوف تعمل على تسطيح الهياكل البيروقراطية الدولية، وتعمل على خلق شبكة أفقية من العلاقات بين الفواعل من الدول ومن غير الدول.

### مستويات انتشار القوة

يشير مفهوم انتشار القوة إلى بعدين من الانتشار؛ هما البعد الداخلي والبعد الخارجي، فيشير الحديث عن انتشار القوة داخل الدولة – أي بمعنى السلطة السياسية Authority – إلى زيادة المشاركة في العملية السياسية وفي عملية صنع القرار، سواء من خلال صياغة القواعد الحاكمة لها أو من خلال التأثير في العملية نفسها[٣٧]، أما البعد الثاني وهو البعد الخارجي لانتشار القوة، فيشير إلى انتقال

(٣٧) Warren J. Samuels, "The Political-Economic Logic of World Governance", Review of Social Economy 59, no. 3 (2001): 273-374.

القوة من التركز في الفاعل الأقوى أو مجموعة من الفاعلين الأكثر قوة في الإقليم أو العالم إلى فاعلين آخرين، سواء كانوا من الدول أو من غير الدول(٣٨).

وهنا يمكن التمييز بين مستويين لانتشار القوة؛ هما: المستوى الأول ويقصد به السلطة التي تتمتع بها الدولة في مواجهة المواطنين، والمستوى الثاني ويقصد به القوة التي تتمتع بها الدولة في مواجهة الدول الأخرى. وعمليًّا فهناك تداخل بين المستويين، فمن ناحية لا ينتج تراجع دور الدولة في الداخل فقط عن تزايد دور الفاعلين المحليين الآخرين داخلها، وإنما ينتج أيضًا عن انتشار القوة بين الفاعلين الخارجين، سواء كانوا من الدول أو من غيرها، وما يترتب على ذلك من تزايد دورهم في المجالات الداخلية المحجوزة تقليديًّا للدولة. ومن ناحية أخرى يمتد تأثر الفاعلين المحليين من غير الدول إلى الخارج بما يسهم في إنهاء احتكار الدولة لدور الفاعل الوحيد في العلاقات الدولية(٣٩).

وفيما يتعلق بالبعد الخارجي لانتشار القوة، هناك اتجاه يبرز سلبيات مثل هذا الانتشار للقوة، باعتباره يهدد استقرار النظام العالمي. فإذا كان النظام ثنائي القطبية، وفقًا لبعضهم، يتسم بدرجة أعلى من اليقين التي تقلل احتمالات الصراع والحروب، مقارنة بالنظام متعدد الأقطاب، فإن النظام القائم على انتشار القوة يحمل احتمالات أكبر لعدم الاستقرار والصراع بأشكال مختلفة(٤٠).

---

(٣٨) Martha Finnemore,"Legitimacy, Hypocrisy, and the Social Structure of Unipolarity: Why Being a Unipole isn't All It's Cracked Up to Be", **World Politics: Quarterly Journal of International Relations 16, no. 1** (Jan 2009): 36-64.

(٣٩) علي جلال معوض، «إعادة الانتشار: تحليل أولي لأبعاد وآثار انتشار القوة داخل وبين الدول»، **ملحق اتجاهات نظرية القوة: كيف يمكن فهم تحولات القوة في السياسة الدولية؟** العدد ١٨٨ (إبريل ٢٠١٢): ١٨-١٩.

(٤٠) المرجع السابق: ٢٢



ولا يمنع ذلك من وجود اتجاه يرى أن انتشار القوة – مثله في ذلك مثل توازن القوى – لا يقوم بالضرورة على التضاد والصراع، بل قد يكون توافقيًا تعاونيًا، أو قائمًا على التكامل. فانتشار القوة أفقيًا ورأسيًا يبني الهياكل الهيراركية القائمة على هيمنة الدول القومية، ويخلق تنظيمات شبكية يستمر في إطارها الدور الأساسي للحكومات والدول، ويتزامن ذلك مع زيادة مكانة الفاعلين الآخرين غير الرسميين، الذين يقوم بعضهم بجانب من أدوار ووظائف الحكومات. ويسهم ذلك في تطوير معايير جديدة للحكم الرشيد، وتقليل سيطرة الحكومات على حياة الأفراد، لا سيما مع زيادة مصادر قوة قطاعات كبيرة من المواطنين، بفعل تمتعهم بالقوة المعلوماتية المرتبطة بتدفق المعلومات وتداولها.

**القوة الإلكترونية وانتشار القوة**

ويتميز الفضاء الإلكتروني بأن له عدة خصائص ساعدت على انتشاره والاعتماد المتزايد عليه؛ منها رخص التكلفة الاقتصادية، والسرعة في تبادل المعلومات، وسهولة استخدامه، فضلاً عن إمكانية تخفي الفاعلين الذين يستخدمونه وعدم الكشف عن هويتهم الحقيقية، وهو ما جعل الفضاء الإلكتروني بيئة جاذبة لمستخدميها، دفعتهم إلى توظيفه في مختلف المجالات السياسية والاقتصادية والاجتماعية والعسكرية.

وكان نتيجة لذلك تنوع وزيادة عدد الفاعلين المستخدمين للفضاء الإلكتروني، وتعدد مجالات استخدامه ووظائفه، فلم يعد يقتصر على تبادل المعلومات؛ حيث يستطيع أحد مستخدمي الفضاء الإلكتروني أن يوقع خسائر فادحة بالطرف الآخر، وأن يتسبب في شل البنية المعلوماتية والاتصالاتية الخاصة



به، وهو ما يسبب خسائر عسكرية واقتصادية، من خلال قطع أنظمة الاتصال بين الوحدات العسكرية بعضها وبعض، أو تضليل معلوماتها أو سرقة معلومات سرية عنها، أو من خلال التلاعب بالبيانات الاقتصادية والمالية وتزييفها أو مسحها من أجهزة الحواسيب. وبالرغم من فداحة الخسائر، فإن الأسلحة بسيطة لا تتعدى الكيلو بايتس، تتمثل في فيروسات إلكترونية تخترق شبكة الحاسب الآلي، وتنتشر بسرعة بين الأجهزة، وتبدأ عملها في سرية تامة وبكفاءة عالية، وهي في ذلك لا تفرق بين المقاتل، والمدني، وبين العام والخاص، وبين السري والمعلوم(٤١).

## الفواعل الدولية وتوظيف القوة الإلكترونية

بداية تجدر الإشارة إلى أن الأفعال وردود الأفعال الدولية والمتمثلة في السياسات والمواقف والاستراتيجيات الخارجية وما يرتبط بها من قرارات وآليات تنفيذية – إنما يقوم بها ويتحمل المسئولية الكاملة عنها من يمكن أن نسميهم بالفاعلين الدوليين. وتشكل سلوكيات هؤلاء الفاعلين على اختلاف دوافعها وتوجهاتها العصب المركزي للنظام السياسي الدولي. كما تؤثر بحسم في مجريات العلاقات السياسية الدولية برمتها.

(٤١) خليفة، «الفضاء الإلكتروني وتهديد الأمن القومي المصري».



## ماذا يقصد بالفاعل الدولي؟

وإذا كان الأمر صحيحًا ولا يثير خلافًا حوله، فإن من ينطبق عليه وصف الفاعل الدولي ضمن الإطار الذي سلف الإشارة إليه، يجب أن يكون محققًا بجملة المعايير الأساسية التالية[٤٢]:

- أن يكون لهذا الفاعل الدولي كيان قابل للتحديد، ويقصد بذلك ألا يكون هذا الكيان هلاميًّا أو هشًّا إلى الحد الذي يصعب معه تحديد ملامحه أو التعرف على خصائصه المميزة، والتي تؤثر بدرجة أو بأخرى في أدائه على المسرح السياسي الدولي.
- وأن يكون حائزًا لذلك القدر من الموارد والإمكانيات الذي يؤهله لاتخاذ القرارات التـي يمكن بها أن يدافع عن مصالحه الأساسية في مواجهة الآخرين. ولا يهم هنا أن تكون الوسيلة إلى ذلك هي التعاون أو التنافس أو الصراع أو الحرب أو غيرها.
- أن تتوافر لديه القدرة على التفاعل مع غيره من الفاعلين الذين يتشاركون معه الأدوار على المسرح الدولي، وبالصورة التي تجعل لهذا التفاعل موقعًا في حساباتهم وتأثيرًا في ما يقيمونه لأنفسهم من توقعات.
- أن يتمتـع بالقدرة على البقاء دون الاستمرار علـى المسرح الدولي لفترة معقولة من الوقت.

وبصورة عامة تتسع قائمة الفاعلين الدوليين والمؤثرين على الساحة الدولية لتشمل[٤٣]:

١- الدول القومية.

٢- المنظمات الحكومية، سواء العالمية أو الإقليمية.

---

(٤٢) إسماعيل صبري مقلد، العلاقات السياسية الدولية: النظرية والواقع، ط. ٤ (د.م: جامعة أسيوط، ٢٠٠٤): ٧٣-٧٥.
(٤٣) المرجع السابق: ٧٥.

٣- الفاعلون فوق القوميين، مثل الاتحاد الأوروبي.

٤- التحالفـات الدولية International alliances، سواء اتخذت طابعًـا سياسيًا أو عسكريًا أو كليهما.

٥- المنظمات الدولية غير الحكومية أو العابرة للقوميات؛ كالصليب الأحمر.

٦- الجماعـات والمنظمات دون مستوى الدول؛ مثل جماعات المتمردين على حكوماتهم وحركات التحرر الوطني والمنظمات الإرهابية.

٧- الشـركات الدوليـة متعددة الجنسية، والتـي أصبحت تمتلك من المـوارد والقدرات ما تفوق إمكانيات بعض الدول.

٨- بعض الأفراد ممن تهيأت لهم دون غيرهم إمكانية التحـرك على قاعدة واسعة نسبيًا من الاتصالات الدولية.

ورغم تعدد استخدامات الفضاء الإلكتروني من الفاعلين الدوليين من الدول وغيرها، فإنه سيتم التركيز على الفواعل من غير الدول؛ كنموذج لانتشار القوة وتراجع سيطرة الدولة على موارد القوة، ومن ثم سيتم التركيز في السطور القادمة على الشركات متعددة الجنسية، والمنظمات الإجرامية، والحركات الإرهابية، وحركات التحرر الوطني، وبعض الأفراد الذين لعبوا دورًا في التفاعلات الدولية عبر الفضاء الإلكتروني وأصبحوا نموذجًا لانتشار القوة من الفواعل من غير الدول. ويتضح ذلك فيما يلي:

## الشركات متعددة الجنسية

أصبحت بعض الشركات متعددة الجنسية تمتلك موارد للقوة تفوق قدرة بعض الدول، ولم يعد ينقصها سوى شرعية ممارسة القوة التي مازالت حكرًا على الدول، فمثلاً خوادم شركات جوجل Google وميكروسوفت Microsoft وأبل Apple المنتشرة في مختلف دول العالم تسمح لها بامتلاك قواعد من البيانات العملاقة، وتستطيع من خلالها استكشاف واستغلال الأسواق، بل والتأثير في اقتصاديات كثير من الدول، وإن أرادت فيمكنها التأثير في قوة الدولة الاقتصادية وقوتها الناعمة أيضًا من خلال تلاعبها بالبيانات والتصنيفات الدولية للاقتصاديات والأسواق؛ حيث تتوجه معظم الدول إلى جذب مثل هذه الشركات الدولية لخلق استثمارات جديدة بها؛ لأن العائد الاقتصادي من تصدير التكنولوجيا مرتفع جدًّا، فمثلا نجد أن ثلثي العائد الاقتصادي لشركة أي بي أم IBM الأمريكية من خارج الولايات المتحدة، على الرغم من أن ربع القوى العاملة بها التي تصل إلى ٤٠٠ ألف موظف من داخل الولايات المتحدة الأمريكية والباقي من مختلف دول العالم[٤٤].

ومن أبرز الأمثلة على قيام الشركات العاملة في مجال الفضاء الإلكتروني بالتأثير في العلاقات الدولية، الصراع بين شركة جوجل والحكومة الصينية؛ حيث قامت الأخيرة باختراق حسابات البريد الإلكتروني Gmail الخاصة بالناشطين السياسيين في الصين. وطالبت شركة جوجل بحجب نتائج البحث حول الموضوعات التي تعتبرها الحكومة الصينية حرجة بالنسبة لها، بما يهدد سمعة

(٤٤) Steve Lohr, "Global Strategy Stabilized IBM During Downturn", New York Times (20 April 2010).

جوجل العالمية خاصة في ظل وجود منافسين أقوياء مثل ميكروسوفت، فضلاً عن سعي الحكومة لسرقة بعض حقوق الملكية الفكرية الخاصة بشركة جوجل، وهو ما دفع الشركة إلى التهديد بالخروج من السوق الصينية إن لم تتوقف الحكومة الصينية عن أفعالها[٤٥]، وقامت بتطوير محرك بحث Baidu الصيني حتى تستطيع الصين الاستغناء عن «جوجل».

أما رد الفعل الأمريكي فقد جاء أكثر حسمًا ووضوحًا مما جعل بعض الخبراء يصفون الأزمة بين جوجل والصين بأنها الحلقة الجديدة في مسلسل التوتر بين واشنطن والصين، والذي يضم خلافات حول الميزان التجاري والمناخ ومبيعات الأسلحة لتايوان وملف حقوق الإنسان.

وقد سارعت إدارة الرئيس الأمريكي باراك أوباما للدفاع عن شركة جوجل؛ حيث أكد المتحدث باسم الرئاسة دعم أوباما الكامل لحرية الإنترنت. كما طالبت هيلاري كلينتون وزيرة الخارجية الأمريكية الصين بتقديم تفسير فيما يتعلق بالاختراقات المذكورة، مؤكدة أن القدرة على العمل بثقة في مجال الإنترنت يعد من الأمور بالغة الأهمية في العصر الحديث[٤٦]، وهو ما دفع الباحث إلى التساؤل عما إذا كان هذا الخلاف جزءًا من الخلاف الأمريكي الصيني أم أنه خلاف تجاري بين الحكومة الصينية والشركة الأمريكية؟

---

(٤٥) Joseph S. Nye, **Cyber Power**: 13–15.

(٤٦) هناء دكروري، «جوجل .. حصان طروادة في الصين»، **جريدة الأهرام** (٢٨ يناير ٢٠١٠).
http://digital.ahram.org.eg/articles.aspx?Serial=197049&eid=1769

وأعلنت شركة جوجل أنه قد تم حجب جميع خدماتها في الصين بما فيها محرك البحث وبريد Gmail وخرائط جوجل، وذلك في الفترة الواقعة من مساء يوم الجمعة ٩ نوفمبر حتى يوم الأحد ١١ نوفمبر، تزامنًا مع المؤتمر الثامن عشر للحزب الشيوعي، الذي يعقد مرة واحدة كل عقد عشر سنوات من أجل تعيين قيادة للحكومة الجديدة(٤٧).

## المنظمات الإجرامية والجريمة الإلكترونية

كما تعتبر المنظمات الإجرامية المتعدية الجنسية، أحد الفواعل الدولية التي تؤثر في التفاعلات الدولية، والتي غالبًا ما تلقى حماية من بعض الحكومات الضعيفة والفاسدة. هذه المنظمات الإجرامية أوجدت لها ساحة على الإنترنت، وأصبحت تقوم بعمليات قرصنة إلكترونية بهدف سرقة المعلومات، أو اختراق حسابات بنكية وتحويل الأرصدة منها، أو من خلال وجود سوق سوداء على الإنترنت لبيع معلومات مالية متعلقة بكلمات مرور شخصية وحسابات بنكية وأرقام كروت وبطاقات ائتمان؛ حيث تكلف الجرائم الإلكترونية الشركات أكثر من ترليون دولار سنويًّا(٤٨). ولما كان من الصعوبة الكشف عن هوية هذه المنظمات؛ لما يتمتع به الفضاء الإلكتروني من قابلية التخفي، فإنه من الصعب مراقبتها أو تتبعها من أجل تقديمها للمحاكمة. وقد قدر التقرير الصادر عن شركة نورتون Norton للأمن الإلكتروني للعام ٢٠١١ أن ٤٣١ مليون شخص

---

(٤٧) «الصين تحجب خدمات «جوجل» عن مواطنيها»، الاقتصادية، http://www.aleqt.com/2012/11/11/article_708496.html

(٤٨) Frederick R. Chang, "Is Your Computer Secure?" Science 325 (July 2009): 550.
http://www.sciencemag.org/content/325/5940/550.short

بالغ يتعرضون للجريمة الإلكترونية سنويًّا، أي أكثر من مليون شخص يقعون ضحية للجرائم الإلكترونية يوميًّا. كما يوضح التقرير أن ٦٤٪ من الأشخاص الذين يقضون ما بين ساعة إلى ٢٤ ساعة في الأسبوع عبر الإنترنت كانوا عرضة للجرائم الإلكترونية[٤٩].

كما أفاد تقرير حكومي رسمي للجرائم الإلكترونية عبر الإنترنت والذي نشر من قبل جامعة الأمن العام الصينية، أنها كلفت الاقتصاد الصينى أكثر من ٤٦ مليار دولار أمريكى فى السنة الماضية، وتحديدًا من شهر يونية ٢٠١١ إلى شهر يونية ٢٠١٢[٥٠].

وهناك أنواع من الجرائم التي يمكن أن تتم بواسطة الفضاء الإلكتروني. وقد يتعرض لها المستخدم، بل قد يكون طرفًا فيها من حيث لا يدري؛ مثلا[٥١]:

- انتحال شخصيات وهمية، أو حقيقية، أو انتحال شخصية الموقع.
- الهجوم على مواقع الإنترنت، والتعديل فيها؛ فقد يدخل أحد المنافسين لموقع شركة منافسة تعرض سلعها، ويتلاعب بالأسعار المعروضة.
- التلاعب في التجارة الإلكترونية؛ حيث يتم استخدام بطاقات الائتمان استخدامًا غير مسموح به. وقد لا يعرف صاحب البطاقة أن بطاقته أصبحت متداولة بين مجموعة من المجرمين، يستنزفونها من حسابه.

(٤٩) «التدرج المروع للجرائم الإلكترونية»، شركة نورتون،
http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimereport/ar-ae/index.html

(٥٠) «جرائم الإنترنت كلفت الصين أكثر من ٤٦ مليار دولار»، موقع المركز العربي لأبحاث الفضاء الإلكتروني،
http://www.accronline.com/article_detail.aspx?id=8296

(٥١) حسن طاهر داود، جرائم نظم المعلومات (الرياض: أكاديمية نايف العربية للعلوم الأمنية، ٢٠٠٠): ٨٣-٩٣.



- وهناك الفيروسات التى تعبث بالأنظمة العاملة، وتعطل الأعمال، وتساعد على خلق البلبلة والاضطراب، وعدم الأمان في استخدامات هذه الوسيلة.
- بالإضافـة إلى الجرائم الأخلاقية من الجنسـ والإعلانات عن الرذائل. وابتزاز بعض الشخصيات.

## الجماعات الإرهابية

ومن أبرز الفواعل الدولية التي أصبحت ظاهرة مُلحَّة بعد أحداث ١١ سبتمبر هي الجماعات الإرهابية؛ حيث كانت من أبرز الجماعات التي استخدمت الإنترنت في عمليات التجنيد والتعبئة، واستغلت الفضاء الإلكتروني كمنبر لنشر أفكارها وجذب مؤيدين ومتطوعين لها، وأصبح المنصة الإعلامية لنشر بياناتها وتعليماتها لمجنديها. وإن لم يتعدَّ الأمر لدى هذه الجماعات مرحلة الدعاية والتجنيد، فإنه يظل بإمكانها اختراق شبكات الكهرباء والطاقة والمواصلات، بل المفاعلات النووية والأسلحة الموجهة إلكترونيًّا أو عبر الأقمار الصناعية والسيطرة عليها أو تدميرها، الأمر الذي قد يسبب كارثة بشرية.

وتعد ممارسة القوة عبر الإنترنت إرهابًا إذا صاحبها دوافع سياسية؛ مثل التأثير في القرارات الحكومية أو الرأي العام. ويتم ذلك من خلال ثلاثة أبعاد هامة؛ فأما البعد الأول فيتمثل في توفير المعلومات عن الأهداف المنشودة لتنفيذ عمليات إرهابية تقليدية، فهو مساعد للإرهاب التقليدي، أو كوسيط في عملية التنفيذ. أما **البعد الثاني** فيستخدم فيه الفضاء الإلكتروني للتأثير في المعتقدات؛ مثل التحريض على بث الكراهية الدينية وحرب الأفكار. أما **البعد الثالث** فيتم في



صورة رقمية؛ حيث تقوم الجماعات المتطرفة على اختلاف أشكالها باستغلال مزايا الفضاء الإلكتروني كعنصر حيوي لدعم وتحقيق أهدافها، ومنفذ لوجستي داعم وحاضن لنشاطها الإعلامي في مناطق مختلفة من العالم(٥٢).

أما عن الطابع العسكري للإرهاب الجديد فيتم استخدام الإنترنت في التنقيب عن المعلومات العسكرية، والحصول على التمويل والتبرعات للقيام بأعمال عسكرية لخدمة أهداف سياسية، فضلاً عن عملية التجنيد والحشد لأتباعها، وكذلك تبادل المعلومات والأفكار والمقترحات والمعلومات الميدانية حول كيفية إصابة الهدف واختراقه وكيفية صنع المتفجرات والتخطيط والتنسيق للعمل الإرهابي، وكذلك في تدمير مواقع الإنترنت المضادة أو اختراق مؤسسات حيوية، أو تعطيل الخدمات الحكومية الإلكترونية أو محطات الطاقة(٥٣).

فبفضل الفضاء الإلكتروني تحولت القاعدة من تنظيم مقيد بإقليم جغرافي وإمكانيات إعلامية محدودة، إلى تنظيم عابر للأقاليم وللحدود ووسائل الإعلام. وقد حصلت القوات الأمريكية على بعض أجهزة الكمبيوتر المحمول الخاصة بأعضاء تنظيم القاعدة في أفغانستان، وقد وجدت عليها نماذج لسدود مائية، ومفاعلات نووية وبعض ملاعب الكرة في أوروبا والولايات المتحدة. وعلى الرغم من وجود دليل على سعي القاعدة لتنفيذ هجمات إلكترونية نحو هذه الأهداف، وأن استخدام الإنترنت كان للتواصل لتنفيذ هجمات إلكترونية نحو

(٥٢) عادل عبد الصادق، «الإرهاب عبر الإنترنت.. تحديات وفرص المواجهة»، المركز العربي لأبحاث الفضاء الإلكتروني، http://www.accronline.com/article_detail.aspx?id=2762

(٥٣) المرجع السابق.



هذه الأهداف[٥٤]، فإن السؤال يظل مطروحًا: ماذا يحدث إذا استطاعت هذه الجماعات توجيه هجمات إلكترونية نحو هذه الأهداف؟

## حركات التحرر الوطني

من أبرز الأمثلة على الفواعل الدولية من غير الدول حركات التحرر الوطني، مثل حركة حماس وحزب الله، وإن كان يشارك هذه الحركات عدد كبير من الأفراد بصفاتهم الشخصية، ويقومون بإرسال هجمات إلكترونية ضد أهداف العدو على الإنترنت، دفاعًا عن قضية. وقد كانت البداية الحقيقة للحرب الإلكترونية بينهما وبين إسرائيل عام ٢٠٠٠، حينما شنت مجموعة إسرائيلية هجمات على موقع حزب الله بعد أسر جنود إسرائيليين؛ حيث قام فريق من القراصنة بحذف محتويات موقع حزب الله ووضع نجمة علم داود وعلم إسرائيل بدلًا منها. وتم الرد على هذا الهجوم الإسرائيلي بهجمات مماثلة على مواقع حكومية إسرائيلية؛ أهمها مكتب رئيس الوزراء وموقع الكنيست وموقع غرفة التجارة وموقع بورصة إسرائيل وموقع بنك إسرائيل. وبلغ عدد المواقع التي تمت مهاجمتها نحو ٢٨٠ موقعًا مقابل ٣٤ موقعًا عربيًّا، كما تعرض أيضًا في ديسمبر ٢٠٠١ ما يقرب من ٨٠ موقعًا إسرائيليًّا لهجمات ناجحة أدت إلى خروجها جميعًا من الخدمة؛ من ضمنها موقع رئيس الوزراء الإسرائيلي، وموقع الجيش الإسرائيلي، وأيضًا تعرض موقع الموساد الإسرائيلي عام ٢٠٠٢ للاختراق وسرقة عملائه الجدد[٥٥].

(٥٤) Gabriel Weimann, Cyberterrorism: How Real Is the Threat? United States Institute of Peace, Special Report (December 2004): 8-9.

(٥٥) «اختراق موقع الموساد في الإنترنت وكشف عملائه الجدد»، جريدة الشرق الأوسط (٢١ اغسطس ٢٠١٣).



وفي إبريل ٢٠١٣ قام مجموعة من الشباب العربي والمسلم بشن حرب إلكترونية على المواقع الإسرائيلية تمكنوا فيها من الحصول على ملفات سرية من خلال اختراق الشبكات وتلغيمها، والحصول على أسماء أفراد من الجيش الإسرائيلي ووحدات وأرقام سرية لمئات من الإيميلات، وحسابات فيسبوك، وحسابات كثيرة لرجال أعمال إسرائيليين، وأكثر من ٥٠٠ حساب مصرفي. كما تم تحميل نحو ألف وثيقة سرية خاصة بالسلطات الإسرائيلية[٥٦].

## الفرد كفاعل دولي

لم يقتصر الأمر على الجماعات الإرهابية والمنظمات الإجرامية، بل أصبح الفرد عنصرًا فاعلًا في التفاعلات الدولية، وأصبح يمارس من الأنشطة عبر الفضاء الإلكتروني ما يؤثر به في العلاقات الدولية. ومن أبرز النماذج على ذلك ظاهرة الويكيليكس "WikiLeaks phenomena"؛ حيث نجح ويليام أسانج في نشر الملايين من الوثائق الخاصة بوزارة الخارجية الأمريكية؛ حيثُ تم استغلال شبكة الإنترنت العالمية في تسريب وثائق تحوي معلومات سرية للغاية مُتداولة بين الإدارة الأمريكية وقُنصلياتها الخارجية بدول العالم، الأمر الذي جعل علاقة الولايات المتحدة مع بعض الدول عرضة للتأثر والتهديد. وقد حكمت المحكمة العسكرية بالولايات المتحدة الأمريكية على الجندي برادلي مانينغ الذي

---

(٥٦) خبر بعنوان: «هاكر جزائري يكشف تفاصيل الحرب الإلكترونية على إسرائيل»، موقع العربية نت، http://www.alarabiya.net/ar/north-africa/algeria/2013/04/10/%D9%87%D8%A7%D9%83%D8%B1-%D8%AC%D8%B2%D8%A7%D8%A6%D8%B1%D9%8A-%D9%8A%D9%83%D8%B4%D9%81-%D8%AA%D9%81%D8%A7%D8%B5%D9%8A%D9%84-%D8%A7%D9%84%D8%AD%D8%B1%D8%A8-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-%D8%B9%D9%84%D9%89-%D8%A5%D8%B3%D8%B1%D8%A7%D8%A6%D9%8A%D9%84.html



قام بتهريب الوثائق لوليام أسانج، بالسجن لمدة ٣٥ عامًا على خلفية تسريب معلومات لموقع ويكيليكس[٥٧].

كما نجح الفضاء الإلكتروني في خلق قنوات اتصال بين بعض المنظمات أو الأفراد وشبكة كبيرة من مستخدمي الفضاء الإلكتروني، خاصة من خلال مواقع التواصل الاجتماعي، التي كان لها دور بارز وهام في تنظيم عديد من المظاهرات في مختلف دول العالم، وكانت بمنزلة نافذة إعلامية دولية لمختلف الأفراد الذين يواجهون انتهاكات حقوق الإنسان، كما ساعد الفضاء الإلكتروني على قيام بعض الأشخاص بارتكاب أعمال قرصنة أو جرائم إلكترونية وسرقة معلومات وبيانات شخصية والتلاعب فيها أو إساءة استغلالها.

ومن أبرز مجموعات القرصنة على الفضاء الإلكتروني مجموعة «أنونيموس Anonymous»؛ وهي مجموعة غير مركزية من القراصنة المنتشرين في العالم، ذات ثقل كبير فيما يسمى بالحرب الإلكترونية، فكانت على سبيل المثال مسئولة عن تسريب آلاف رسائل البريد الإلكتروني الخاصة بالرئيس السوري بشار الأسد. كما هاجمت مواقع حكومية أمريكية وبريطانية وأخرى للناتو قبل أن تعلن مؤخرًا مهاجمتها لمواقع حكومية إسرائيلية تعاطفًا مع أهالي قطاع غزة الذين يتعرضون لحملة عسكرية جديدة. وقد تأسست المجموعة عام ٢٠٠٣ عبر منتدى "chan4"، الذي يعرض الأعضاء فيه مشاركاتهم دون الإشارة إلى هويتهم ولا يتطلب التسجيل للمشاركة فيه، لتمثل المجموعة حسب تصورها الدماغ

(٥٧) «أمريكا: السجن ٣٥ عامًا لمسرب ويكيليكس»، CNN بالعربية،
http://arabic.cnn.com/2013/world/8/21/nning-Sentencing-Courtroom-URGENT-1/index.html



الرقمي العالمي الفوضوي لمجتمع مستخدمي الإنترنت الذين يوجدون في وقت واحد، ويتبنون مبدأ المعارضة الشديدة للرقابة على الإنترنت[٥٨].

وقد قامت مجوعة أنونيموس باختراق بيانات شخصية؛ بينها أرقام بطاقات ائتمان تخص آلافًا من عملاء شركة تختص بتحليل المخاطر الاقتصادية والسياسية والعسكرية. وقالت المجموعة في بيان لها: إنه من بين العملاء التي اخترقت حساباتهم وزارة الدفاع الأمريكية وأجهزة أمنية رسمية ومتعاملون أمنيون ومنظمات إعلامية[٥٩].

ومن ثم نصل إلى نتيجة مفادها أن الفضاء الإلكتروني ساعد على انتشار القوى بين مختلف الفاعلين، وأعطى مساحة متزايدة للفواعل من غير الدول للتأثير في التفاعلات الدولية. وكان نتيجة لهذا الانتشار أن زادت المخاطر والتهديدات التي تواجهها الدول عبر الفضاء الإلكتروني، وأصبح من الضروري امتلاك مصادر التكنولوجيا الحديثة التي تمكن الدول من مواجهة هذه المخاطر، بل امتلاك الأسلحة الإلكترونية التي يتم استخدامها.

(٥٨) «أنونيموس .. القراصنة المجهولون»، موقع الجزيرة،
http://www.aljazeera.net/news/pages/063 cb2e9-5134-4509-a278-6eab43f8bd65?GoogleStatID=9

(٥٩) «قراصنة كمبيوتر يسرقون معلومات شخصية من شركة أمنية أمريكية»، BBC،
http://www.bbc.co.uk/arabic/scienceandtech/2011/12/111225_hackers_us_security.shtml

## المبحث الثالث

## عناصر القوة الإلكترونية وأبعاد استخدامها في التفاعلات الدولية

لم تعد تسيطر تلك النظرة التقليدية التي ترى أن الفضاء الإلكتروني هو مجال لتبادل المعلومات فقط، فبعد أحداث ١١ سبتمبر ٢٠٠١ بدأ التركيز على الفضاء الإلكتروني كتهديد أمني جديد بفعل أحداث دولية، كان أبرزها استخدام تنظيم القاعده له كساحة قتال ضد الولايات المتحدة. وفي عام ٢٠٠٧ برز بوضوح دور الفضاء الإلكتروني كمجال جديد في العمليات العدائية في الصراع بين روسيا واستونيا، وكذلك في عام ٢٠٠٨ في الحرب بين روسيا وجورجيا. وجاء الهجوم بفيروسي «ستاكسنت Stuxnet» عام ٢٠١٠ و«فليم Flame» عام ٢٠١٢ على البرنامج النووي الإيراني ليمثل نقطة هامة في تطور الأسلحة الإلكترونية. وعلى الرغم من الدور السياسي الذي لعبته مواقع التواصل الاجتماعي في حالة الثورات العربية في مطلع عام ٢٠١١، فإنها مثلت نقطة هامة لدعم الاهتمام الدولي بأمن الفضاء الإلكتروني، وبرزت محاولات للسيطرة عليها بعد تصاعد الاحتجاجات في أكثر البلدان ديمقراطية؛ وهي بريطانيا والولايات المتحدة الأمريكية[٦٠].

---

(٦٠) عادل عبد الصادق، «القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني»، سلسلة قضايا استراتيجية، المركز العربي لأبحاث الفضاء الإلكتروني (أكتوبر ٢٠١٢): ٢.



## عناصر القوة الإلكترونية

كان نتيجة لاتجاه الصراع الدولي حول الموارد والمصالح والقيم نحو الاعتماد المتزايد على تكنولوجيا الاتصال والمعلومات أن أصبح الفضاء الإلكتروني ساحة جديدة للصراع بشكله التقليدي، ولكنه ذو طابع إلكتروني يتجاوز الحدود القومية وسيادة الدول. ويسعى كل طرف من طرفي الصراع إلى تحقيق أكبر مكاسب وإلحاق أكبر قدر من الخسائر بالطرف الآخر. ويتميز الصراع الإلكتروني بأن به تدميرًا لا يصاحبه دماء أو أشلاء، ويتضمن التجسس والتسلل ثم النسف، لكن لا دخان ولا أنقاض ولا غبار، وتتميز أطرافه بعدم الوضوح وتكون تداعياته خطيرة، سواء عن طريق تدمير المواقع على الإنترنت ونسفها، أو قصفها بوابل من الفيروسات، أو العمل على استخدام أسلحة الفضاء الإلكتروني المتعددة للنيل من سلامة تلك المواقع، وهي أسلحة يسهل الحصول عليها من خلال مواقع الإنترنت وتعلم كيفية استخدامها(٦١).

ونتج عن ذلك ظهور شكل جديد من الحروب، يكون في وسط الشعوب، بعيدًا عن الساحات التقليدية للصراع الدولي، هذا الشكل هو «الحرب الإلكترونية».

ويُنظر إلى الحرب الإلكترونية على أنها تعني القدرة على الدفاع عن والهجوم على المعلومات من خلال شبكات الحاسب الآلي عبر الفضاء الإلكتروني، بالإضافة إلى شل قدرة الخصم على القيام بنفس هذه الهجمات؛ حيث يرى كينث جريس أن الحرب الإلكترونية تشمل خمسة عناصر رئيسية؛ هي:

(٦١) المرجع السابق: ٢-٤.



التجسس، والدعاية، والحرمان من خدمة الإنترنت، وتعديل البيانات والتلاعب بها، والتلاعب أيضًا بالبنية التحتية(٦٢).

وتتركز عناصر القوة الإلكترونية لدولة ما في ثلاثة محاور رئيسية؛ هي:

- بنية تكنولوجية Cyber Infrastructure
- الأسلحة الإلكترونية Cyber weapons
- العمليات الإلكترونية Computer Network Operation (CNO) والتي تشمل:
  - مهاجمة شبكات الحاسب الآلي Computer Network Attack (CNA)
  - الدفاع عن شبكات الحاسب الآلي Computer Network Defense (CND)
  - استطلاع شبكات الحاسب الآلي Computer Network Exploitation (CNE)

## أولاً: بنية تكنولوجية

وهي بمنزلة البنية التحتية اللازمة للقوة الإلكترونية، فبدلاً من الدبابات والطائرات والغواصات، تحتاج الدولة في هذا النوع إلى أجهزة كمبيوتر، وشبكات اتصالات مرتبطة بأجهزة الكمبيوتر بعضها ببعض، وبرمجيات، بالإضافة إلى العنصر البشري المدرب على استخدام هذه الأجهزة والشبكات. وكما تمارس الدولة نوعًا من التأثير في الإقليم البري والإقليم الجوي والإقليم البحري من خلال قوتها العسكرية المادية، تستطيع أن تمارس أيضًا من خلال بنيتها المعلوماتية والتكنولوجية نوعًا من التأثير في الفضاء الإلكتروني(٦٣).

---

(٦٢) Kenneth Geers, **Cyber Space and the Changing Nature of Warfare** (U.S. Representative to the Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia), **DIME**, http://www.carlisle.army.mil/DIME/CyberSpace.cfm On 15 August 2013

(٦٣) Miller and Kuehl, "Cyberspace and the 'First Battle' in 21st-century War", **Cyberwarfare and Cyberterrorism: The Need for a New U.S. Strategic Approach** (Washington, DC: Cyber Secure Institute, 2010): 2.



## ثانيًا: الأسلحة الإلكترونية

وهي برامج تم تصميمها للقيام بوظائف مختلفة؛ وتشمل:

١- فيروسات الحاسوب Viruses

وهي برامج خارجية صُنعت عمدًا بغرض تغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر، إما بالإزالة وإما التعديل وإما التخريب وما شابهها من عمليات، أي أن الغرض منها هو إلحاق الضرر بحاسوب آخر أو السيطرة عليه، وتتم كتابتها بطريقة معينة. وقد تستخدم الفيروسات لتعطيل شبكات الخدمات والبنية التحتية لطرف المستهدف؛ كأن يتم عن طريقها إحداث فشل في شبكة الاتصالات لدولة ما[٦٤].

٢- الديدان Worms

هي برامج صغيرة لا تعتمد على غيرها وتتكاثر بنسخ نفسها عن طريق الشبكات، صنعت للقيام بأعمال تخريبية؛ كأن تعمل على قطع الاتصال بالشبكة أو سرقة بعض البيانات الخاصة بالمستخدمين أثناء تصفحهم للإنترنت، وتمتاز بسرعة الانتشار ويصعب التخلص منها؛ نظرًا لقدرتها الفائقة على التلون والتناسخ والمراوغة. وغالبًا عندما تستخدم في حروب المعلومات تستهدف الشبكات المالية التي تعتمد على الحاسوب؛ مثل شبكات البنوك[٦٥].

٣- أحصنة طروادة Trojan horses

هي شفرة أو برنامج صغير مختبئ في برنامج كبير من البرامج ذات الشعبية العالية، ويقوم ببعض المهام الخفية كأن يعمل على نشر دودة أو فيروس، وهو

---

(٦٤) "What do Computer Viruses do?" **Microsoft,**
http://www.microsoft.com/security/pc-security/virus-whatis.aspx

(٦٥) **Viruses or Hoaxes,** http://virusall.com/computer%20worms/worms.php



مبرمج بمهارة عالية؛ إذ لا يمكن اكتشاف وجوده؛ حيث يعمل دائمًا على مسح آثاره التي لا تحمل صفة تخريبية. وغالبًا ما يعمل على إضعاف قوى الدفاع لدى الضحية ليسهل اختراق جهازه وسرقة بياناته؛ كأن يقوم مثلاً بإرسال بيانات عن الثغرات الموجودة في نظام ما، وكذلك إرسال كلمات المرور السرية الخاصة بكل ما هو حساس من مخزون معلومات الطرف المستهدف(٦٦).

٤- القنابل المنطقية Logic bombs

تعد نوعًا من أنواع أحصنة طروادة؛ حيث يزرعها المبرمج داخل النظام الذي يطوره، وقد تكون برنامجًا مستقلًا وتُصمم؛ بحيث تعمل عند حدوث أحداث معينة أو تحت ظروف معينة أو لدى تنفيذ أمر معين، وتؤدي إلى تخريب أو مسح بيانات أو تعطيل النظام لطرف المستهدف(٦٧).

٥- الأبواب الخلفية Backdoors

هي ثغرة تُترك عن عمد من قبل مصمم النظام؛ لكي يستطيع الدخول إلى النظام عند حاجته لذلك؛ حيث تقوم كبرى الدول المصدرة للبرمجيات بترك أبواب خلفية تستخدمها عند الحاجة، وهو ما يمكن هيئات وأركان حرب المعلومات من التجوال الحر داخل أي نظام لأية دولة أجنبية(٦٨).

٦- الرقائق Chipping

من الممكن أن تحتوي بعض الرقائق الإلكترونية على وظائف غير متوقعة أو معروفة كما في البرامج والنظم؛ حيث يمكن للدوائر المجمعة التي تشكل

---

(٦٦) "Information Security Information, News and Tips", SearchSecurity, http://searchsecurity.techtarget.com/definition/

(٦٧) Ibid.

(٦٨) Ibid.



هذه الرقائق أن تحتوي على وظائف إضافية أثناء تصنيعها، لا تعمل في الظروف العادية، إلا أنها قد تعلن العصيان في توقيت معين، أو بالاتصال بها عن بعد؛ حيث يمكن أن تستجيب لتردد معين لبعض موجات الراديو، فتشل الحياة في مجتمع أو دولة ما(٦٩).

٧- الماكينات والميكروبات فائقة الصغر

ويطلق عليها (Nano machines and Microbes)، وهي عكس الفيروسات؛ حيث إنها تصيب عتاد النظام (Hardware) فالـ (Nano machines)عبارة عن(robots) فائقة الصغر قد تنتشر في مبنى نظام معلوماتي في دولة معادية أو منافسة؛ حيث تتفشى في الطرقات والمكاتب حتى تجد حاسبًا آليًا، وتدخل إليه من خلال الفتحات الموجودة به، لتبدأ عملها بإتلاف الدوائر الإلكترونية.

أما الميكروبات (Microbes) فمن المعروف أن بعضًا منها يتغذى على الزيت، فماذا لو تم تحويرها جينيًا لتتغذى على عنصر الـ (silizium) المكون الهام في الدوائر الإلكترونية؟ إن هذا يعني تدمير وإتلاف الدوائر الإلكترونية في أي معمل يوجد فيه حاسبات آلية أو حاسب خادم (server) لموقع على الإنترنت، أو مبنى هام أو حساس يدار بالكمبيوتر، أو حتى مدينة بأسرها؛ عن طريق إتلاف دوائر التحكم الإلكترونية فيها.

٨- مدافع HERF

عبارة عن مدافع تطلق موجات راديو مركزة وعالية الطاقة والتردد (High Energy Radio Frequency)، والتي يمكنها تعطيل وإتلاف أي هدف إلكتروني. أما

---

(٦٩) Ibid.

مستويات الضرر التي قد تحدثها فهي تختلف من ضرر متوسط؛ كغلق شبكة حاسب مثلاً أو إعادة تشغيله بشكل دوري فلا يمكن استغلاله، إلى ضرر بالغ كإعطاب العتاد الخاص بالحاسب أو الشبكة بشكل لا يمكن بعده إصلاح الحاسب أو الشبكة(٧٠).

٩- قنابل EMP

هي تشبه المدافع غير أنها تستخدم نبضات إلكترومغناطيسية (Electromagnetic Pulse)؛ حيث يمكن التسلل إلى مواقع العدو الإلكترونية الحساسة والهامة وإلقاء هذه القنابل التي سوف تتلف كل الحواسب والشبكات في دائرة انفجارها غير المدوي أو المشتعل، وهي وإن كانت أصغر حجمًا من مدافع (HERF)، فإنها أوسع وأبعد أثرًا؛ حيث إنها لا تنتقي هدفًا معينًا، بينما قذيفة مدفع (HERF) تنتقي هدفها(٧١).

## ثالثًا: العمليات الإلكترونية

وتنقسم إلى ثلاثة أنواع رئيسية؛ هي:

أولًا: مهاجمة شبكات الحاسب الآلي (Computer Network Attack, (CNA: وتشمل اختراق الشبكات لحقن الحاسبات بكمٍّ هائل من البيانات لتعطيلها أو وضع بيانات ومعلومات محرفة لإرباك مستخدمي الحاسبات، ونشر الفيروسات (Viruses) وما شابهها من البرامج الصغيرة المؤذية؛ مثل الديدان(Worms)، وتلغيمها بالقنابل المنطقية (Logic Bombs) التي يتم تنشيطها في الوقت المناسب للمهاجم؛ لكي

(٧٠) Mike Nathan, **HERF gun zaps more than your dinner** http://hackaday.com/2011/03/21/herf-gun-zaps-more-than-your-dinner/ On 20 July 2013

(٧١) "“EMP 101” A BASIC PRIMER & SUGGESTIONS FOR PREPAREDNESS", **Onesecondafter.Com,** http://www.onesecondafter.com/pb/wp_d10e87d9/wp_d10e87d9.html

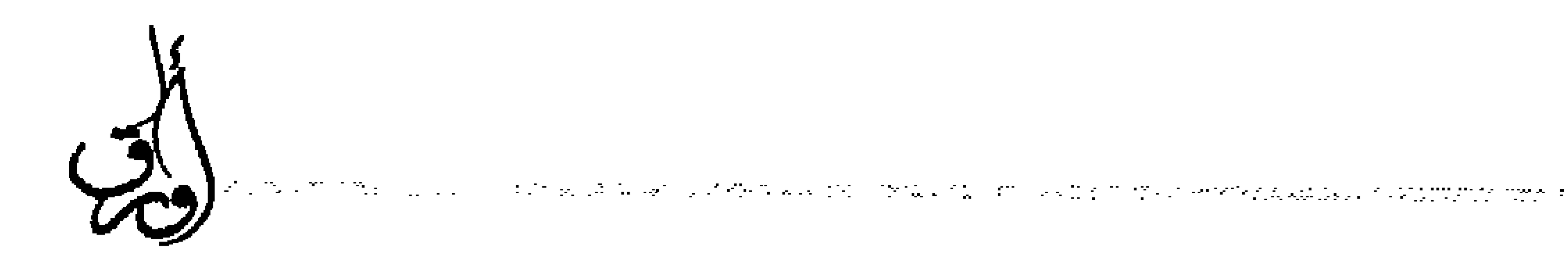


تتلف ما تحتويه الحاسبات من بيانات وبرمجيات، أو القيام بهجمات إلكترونية أو مادية لقطع لخدمات الإنترنت (denial of service attacks) عن الخصم، ومن ثم القدرة على تدمير قواعد البيانات الإلكترونية التي يمتلكها، وتعطيل قدرته على النشر السريع لقدراته وإمكانياته وقواته، أو قطع أنظمة الاتصال بين الوحدات العسكرية وبعضها وتعطيل شبكات الكمبيوتر، أو شل أنظمة الدفاع الجوي أو التوجيه الإلكتروني للخصم، أو السيطرة على وحدات القيادة والتوجيه، أو فقدان العدو قدرته على التحكم أو الاتصال بالأقمار الصناعية(٧٢)، وقد يصل الأمر إلى التدمير الفعلي (Physical Destruction) من خلال تدمير الجانب المادي؛ مثل الخادمات والأسلاك والكابلات والأجهزة التي تحتوي على المعلومات؛ حيث يصعب التأثير فيها من بعد. وتتم عملية التدمير بالأسلحة التقليدية؛ كالجوية والبحرية والبرية أو بعمليات القوات الخاصة.

ثانيًا: الدفاع عن شبكات الحاسب الآلي (Computer Network Defense (CND:
وتشمل هذه العملية حماية الشبكات وأجهزة الكمبيوتر من أية عملية اختراق خارجي. ويجب أن يكون التأمين على مستوى البرمجيات (Software) والمكون المادي للشبكات (Hardware)؛ بحيث يتم تأمين الشبكة من أي اختراق خارجي بأيٍّ من الأسلحة الإلكترونية السابق ذكرها، وكذلك تأمين المكون المادي للشبكات؛ مثل الخوادم أو الشرائح الإلكترونية، والتي قد تكون مبرمجة من قبل المصمم؛ لكي تعمل في ظروف غير عادية لصالحه(٧٣).

(٧٢) Colonel Jayson M. Spade, **China's Cyber Power And America's National Security**, edited by Jeffrey L. Caton (U.S.: Army War College, 2012): 7.

(٧٣) Ibid: 9.



ثالثًا: استطلاع شبكات الحاسب الآلي (CNE) Computer Network Exploitation:
وتعني القدرة على الدخول غير المشروع والتجسس على شبكات الخصم، دون أن يصاحب ذلك تدمير أو تخريب للبيانات والمعلومات، بهدف الحصول على هذه المعلومات، والتي قد تشمل خطط دفاع وهجوم عسكري، أو أسرارًا عسكرية وحربية، أو معلومات سياسية واستخباراتية. ولا تتوقف وظيفتها على ذلك فحسب، بل يمكن من خلالها عمل خرائط لشبكات الحاسب الآلي واستخدامها مستقبلًا في عمليات الهجوم الإلكتروني. كما يمكن ترك بعض الثغرات من خلال الأبـواب الخلفية (Backdoors) لحقن الشبكة بفيروسات للقيام بمهام معينة؛ مثل نقل البيانات إلى أجهزة المتجسس(٧٤). كما يمكن أيضًا استخدامها في التأثير في أفكار وسلوكيات الخصم من قبيل الحرب النفسية، وذلك بنشر مثل هذه الخطط العسكرية والبيانات أو إرسالها إليه مرة أخرى؛ لكي يدرك إلى أي مدى هو مُخترق ولن يستطيع المواجهة، مما يدفعه إلى الاستسلام أو التفاوض.

## استخدامات القوة الإلكترونية في التفاعلات الدولية

تصاعد الاهتمام الدولي بالفضاء الإلكتروني، خاصة بعد ما أتاحه من أدوات وآليات جديدة كوسيلة ووسيط لتهديد عمل المرافق الحيوية والبنية التحتية الكونية للمعلومات وعدم توقفها أمام سيادة الدول، بما جعلها بيئة خصبة للاستخدام غير السلمي من جانب كافة الفاعليين على تنوعاتهم المختلفة والذين تراوحوا

(٧٤) Dennis M. Murphy, ed., Information Operations Primer (Carlisle: U.S. Army War College, 2010): 169.



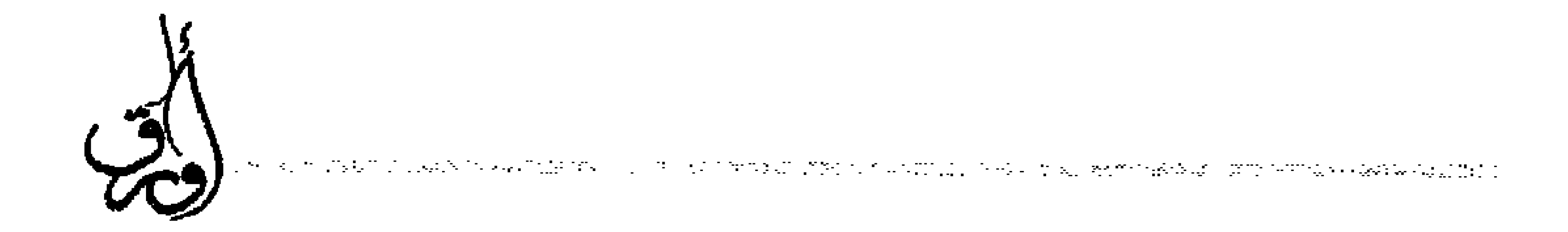
ما بين استخدام الدول إلى الفاعليين من غير الدول. وظهر ذلك في استخدام الفضاء الإلكتروني كساحة للحرب الباردة والحرب النفسية وحرب الأفكار، أو من خلال استخدامه لشن الحروب والإرهاب بين الدول أو استخدام الأفراد أو الجماعات الإرهابية أو القراصنة أو الجريمة المنظمة، وذلك على نحو يؤثر في الطبيعه المدنية أو السلمية للفضاء الإلكتروني.

وقد حدد جوزيف ناي أنماطًا لاستخدام القوة الإلكترونية، وميز بين الاستخدام الناعم لها والاستخدام الصلب. ويمكن توضيح ذلك من خلال الآتي:

**١- القوة الإلكترونية والقوة الصلبة**

- تتنوع مظاهر الاستخدام الصلب للقوة الإلكترونية في التفاعلات الدولية؛ حيث يتم استخدام القوة الإلكترونية في التأثير في سلوكيات الفاعل الدولي، ودفعه للقيام بأعمال لم يكن ليقوم بها. ويتم تحقيق ذلك من خلال نشر فيروسات تدمر أجهزة الدولة، وتستهدف نظم الكمبيوتر الخاصة بالخدمات الحكومية(٧٥)، أو من خلال الحرمان من خدمة الإنترنت، أو قطع خدمات الإنترنت عن الدولة كاملة، فعلى سبيل المثال تم شن هجمات على البرنامج النووي الإيراني للعمل على تعطيله؛ حيث أعلنت الاستخبارات الإيرانية أن فيروس ستاكسنت أصاب حوالي ١٦ ألف جهاز كمبيوتر. ولم يكتف الأمر بذلك فقط؛ حيث تم استخدام فيروسات أكثر تعقيدًا مثل فيروس (flim) لتعطيل البرنامج النووي والتجسس عليه.
- كما يتم استخدامها أيضًا للتحكم في أجندة الآخرين من خلال إقصاء بعض استراتيجياتهم، ويتضح استخدام الفضاء الإلكتروني في ممارسة القوة الصلبة في

(٧٥) Joseph s. Nye, **The Future of Power**, speech before Pacific Forum (March 2011).



هـذا الوجه عندما دشنـت الحكومة الأمريكيـة موقعًا على الإنترنـت بمنزلة سفارة إلكترونية لتزويـد الإيرانيين بمعلومات حول التأشيرات عبر الإنترنت وللتواصل مع الطـلاب الإيرانيين، مما دفع الحكومـة الإيرانية إلى حجب الموقع وتجريم محاولة الدخول عليه(٧٦).

- كما يتم توظيف القوة الإلكترونية في ترتيب أولويات الفواعل الأخرى؛ حيث قامت الولايات المتحـدة الأمريكية باتخاذ عدة إجراءات ضـد شركات بطاقات الائتمان لمنع ممارسة القمار عبر الإنترنت.

## ٢- القوة الإلكترونية والقوة الناعمة

- أما فيما يتعلق بالاستخدام الناعم للقوة الإلكترونية فيمكن من خلال التأثير في سلوك الفاعل؛ مثل استخدام موقع اليوتيوب في تخطي أسوار التعتيم التي تفرضها الأنظمة المستبـدة وفضح الانتهاكات التي ترتكبها أمـام العالم. كما حدث في عام٢٠٠٧، عندمـا استخدمت كاميرات المحمـول لتصوير قمع النظـام العسكري الحاكم في ميامـار (بورما سابقًا) للمظاهرات المطالبة بالديمقراطيـة، وتم بثها على الإنترنت. وهـو مـا تكرر مع إيران عقـب الانتخابـات الرئاسية، بهدف خلـق رأي عام دولي للضغط على هذه الحكومات للاستجابة لمطالب الشعوب.
- ويتم استخدامها أيضًا للتحكم في أجندة الآخرين، ومن أمثلة ذلك بعض الشروط التي تضعهـا منظمة الأيكان على أسماء نطاقات الإنترنـت، وكذلك المعايير الموضوعة والتي لاقت قبولًا واسعًا لتصميم واستخدام البرمجيات(٧٧).

---

(٧٦) عبد الصادق، «القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني» : ٩.

(٧٧) Joseph S. Nye, **Cyber Power**: 7–9.



كما يتم استخدامها لترتيب أولويات الآخرين من خلال العمل على نشر أو تقييد قيم وثقافات عبر الإنترنت؛ مثل تطوير قيم رافضة لنشر الإباحية عبر الإنترنت.

**القوة الإلكترونية والصراع الدولي**

تطور الصراع الدولي بشكل هائل نتيجة للتطور الكبير في المعلومات مما جعل هذهِ المعلومات هي الهدف الأساسي الذي تسعى الدول للحصول عليه، فقد مكنَت المعلومة الدول من إنتاج السلاح النووي. وظل هذا التطور مستمرًّا؛ حيث اعتمدت كل مرحلة من مراحل التطور الإنساني على سلطة أو قوة من طبيعة معينة تتناسب مع متطلبات هذه المرحلة. ولقد أثرت هذه السلطة أو القوة بصورة مباشرة أو غير مباشرة في أدوات الصراع بين المجتمعات وآلياتها، وأفرزت مفردات ومكونات تكاملت معًا لتنتج نظامًا دوليًّا سيطرت مفاهيمه بعض الوقت أو كل الوقت. وفي هذا الإطار تميز عصرنا الحالي بظاهرة الثورة العلمية والتكنولوجية. ولقد أزاحت وحيّدت التكنولوجيا كثيرًا من عناصر القوة عن مواقعها التي تربعت عليها فترة طويلة، مما عرض المفهوم التقليدي للقوة إلى انتقادات. وأفصح عن محتوى جديد للقوة؛ فلم يعد ما في يد الدولة من قدرات عسكرية أو ما تمتلكه من أموال وثروات، كافية لبلورة دورها كقوة مؤثرة وفاعلة. إن مسار هذا التغير الذي أحدثته التكنولوجيا في حالة حركة وهو في طريقه إلى التصاعد وطور التكوين. ومن غير الممكن فهم العلاقات الدولية وظاهرة الصراع الدولي بمعزل عن التطور الذي يشكل ملمحًا لم يكتمل بعد؛ حيث يصعب تحديد آثاره وتداعياته بشكل شامل ونهائي حاليًّا ومستقبلاً[٧٨].

(٧٨) إيهاب عبد الحميد خليفة، «القوة الإلكترونية والصراع الدولي»، المركز العربي لأبحاث الفضاء الإلكتروني، http://www.accronline.com/print_article.aspx?id=15636

ومع بروز الفضاء الإلكتروني زادت الرغبة في السيطرة عليه باعتباره ميدانًا جديدًا للعلاقات والتفاعلات بين الدول والفاعلين من غير الدول، وأصبح سلاحًا ذا حدين، فقد يتطور الخلاف السياسي بين دولتين إلى مواجهة عبر الفضاء الإلكتروني، وقد يتطور إلى إحداث أضرار مادية ضخمة، وهو ما يمثل مكمن الخطورة الأكبر في درجة التأثير على الصراع الدولي، خاصة في الوقت الذي تسعى فيه جميع الدول إلى الحصول على المعلومة واقتحام أنظمة المعلومات السرية للأجهزة العسكرية والمعلوماتية. إلا أنه يلعب في نفس الوقت دورًا في المساعدة على منع الصراعات؛ وذلك من خلال المساعدة على تقريب وجهات النظر وتبادل الأفكار والرؤى والآراء؛ حيث يشهد الفضاء الإلكتروني عبر الشبكات الاجتماعية والتجمعات الإلكترونية زيادة العلاقات بين المواطنين عبر الدول، وسهولة تبادل المعلومات والبيانات، والمساعدة على تجاوز الهياكل البيروقراطية للحكم. كما عزز الفضاء الإلكتروني من التغيير الهيكلي للدبلوماسية؛ بالانتقال الجزئي من الاعتماد على الدولة الرسمية إلى تفاعل جهات وجماعات وأفراد داخل الدولة، والانتقال من مرحلة تبني النموذج المركزي في صنع السياسة الخارجية للانفتاح على طرق تنفيذ أهدافها، وتم تنشيط الاتصالات الداخلية ووزارة الخارجية والانفتاح على المعلومات .

يأخذ الصراع الإلكتروني طابعًا تنافسيًا حول الاستحواذ على سبق التقدم التكنولوجي وسرقة الأسرار الاقتصادية والعلمية إلى أن يمتد ذلك الصراع إلى محاولة السيطرة على الإنترنت؛ من خلال السعي للسيطرة على أسماء النطاقات وعناوين المواقع والتحكم بالمعلومات والعمل على اختراق الأمن القومي للدول بدون استخدام طائرات أو متفجرات أو حتى انتهاك للحدود السيادية كهجمات



قراصنة الكمبيوتر وتدمير المواقع والتجسس، لما يكون له من تأثير في تدمير الاقتصاد والبنية التحتية بنفس القوة التي قد يسببها تفجير تقليدي مدمر(٧٩).

**وللصراع الإلكتروني خصائص تميزه؛ هي:**

- الفاعلون الدوليون متنوعون وفي بعض الأحيان مجهولون.
- غير مكلف ماديًّا أو ماليًّا.
- سهولة البداية والانتهاء.
- بـه جزء مادي متمثل في خضوع الأجهزة والسرفـرات والحاسبات لسلطان الدولة وسيادتها.
- قابلية تغيير الخصائص مستقبلاً نتيجة التغيرات السريعة في التكنولوجيا.
- الغالبية العظمى لا تستطيع نزع سلاح الطرف الآخر أو تدميره كليًّا أو احتلال إقليمه.
- إمكانية استخدام الفضاء الإلكتروني في القوة الناعمة أو القوة الصلبة.

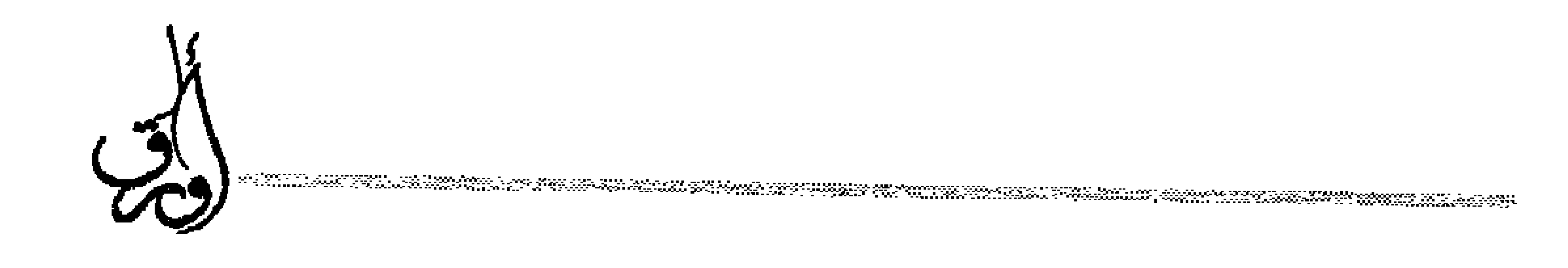
## الردع الإلكتروني والأمن الدولي

هدف الردع هو خلق مجموعة من محفزات المناعة لقيام أحد أطراف الصراع من القيام باعتداء أو هجوم مستقبلاً(٨٠)، وإذا كان ذلك هو هدف الردع في التفاعلات الدولية على أرض الواقع، فإنه مختلف جزئيًّا في حالة الردع الإلكتروني؛ لأن أحد الفواعل غير قادر على إزالة أو تدمير الطرف الآخر كليًّا، كما في حالة الردع النووي مثلًا.

---

(٧٩) عبد الصادق، «القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني»: ٥.

(٨٠) Martin C. Libicki, **Cyberdeterrence and Cyberwar** (Santa Monica: RAND, 2009): 28.



كما أنه ليس من السهولة تحقيق الردع الإلكتروني بسبب خاصية التخفي، التي تمنع مستخدم القوة الإلكترونية من التعرف على خصمه أو التوقع من أين سوف تأتيه الضربة، وهو ما يطرح سؤالًا حول إمكانية أن تقوم الهجمات الإلكترونية بتهديد السلم والأمن العالميَّين.

وفي ظل نظام دولي يتميز بتعدد القطبية، مما يزيد من احتمالات الصراع، فضلاً عن تعدد الفاعلين من الدول وغير الدول الذين يستخدمون القوة الإلكترونية في التفاعلات الدولية، بالإضافة إلى خاصية التخفي، فإن احتمالات الصراع الدولي تزداد.

ومن خلال تتبع بعض النماذج: مثل الحرب بين روسيا وأستونيا عام ٢٠٠٧ وبين روسيا وجورجيا عام ٢٠٠٨، والاعتداء على البرنامج النووي الإيراني، واستخدام الفضاء الإلكتروني في عمليات التعبئة والتجنيد والحشد والحرب النفسية والإعلامية، نجد أن القوة الإلكترونية أصبحت تستخدم إلى جانب القوة العسكرية، بل أصبحت أحد المبادئ الهامة في أية استراتيجية عسكرية.

## القوة الإلكترونية وسباق التسلح

للتسليح أهمية استراتيجية مؤثرة في توازن القوى وبسط النفوذ وتمكين الدول من ممارسة عديد من الأدوار والضغوط والتكتلات في ظل بيئة أمنية يمتلكها الشك وعدم اليقين ومصالح استراتيجية قابلة للتدمير في ثوان معدودة، واتجهت الدول لتعزيز دفاعاتها ضد خطر التعرض للهجمات الإلكترونية، ولكن الاتجاه الأكثر خطورة هو التحول من اتخاذ إجراءات وقائية ذات طابع دفاعي



إلى الاتجاه إلى تبني سياسات هجومية، وهو ما يحمل خطورة عسكرة الفضاء الإلكتروني دون الأخذ بعين الاعتبار كونه يختلف عن ظروف التقدم في امتلاك الأسلحة النووية أو البيولوجية، ودون الأخذ بالاعتبار حجم التدمير المنتظر وقوعه حال التعرض لهجوم إلكتروني، وهو ما يمثل خطورة خاصة مع السعي إلى تطوير هذه الأسلحة ونشرها في ساعات.

وعلى الرغم من سرية النشاط المتعلق بالقدرات الإلكترونية، فإن التوقعات تشير إلى أن هناك ما لا يقل عن ١٢٠ دولة تقوم بتطوير طرق للتجسس واستخدام الإنترنت؛ كسلاح لاستهداف أسواق المال ونظم الكمبيوتر الخاصة بالخدمات الحكومية. ومن أهم الدول التي تمتلك قدرات هجوم إلكترونية الولايات المتحدة، والصين، وروسيا،وإسرائيل، وفرنسا، وبريطانيا،والهند، وألمانيا[٨١].

وقد دفع عجز حلف الناتو في مواجهة الهجمات الإلكترونية على أستونيا وجورجيا إلى تكوين وحدة للدفاع الإلكتروني، مقرها تالين عاصمة أستونيا، وعمل على تطوير المفهوم الاستراتيجي للحلف؛ بحيث أصبح الفضاء الإلكتروني منطقة لعمليات الحلف، وأن عليه أن يطور قدراته الدفاعية الإلكترونية بما يشمل مساندة ودعم حلفائه الذين يتعرضون لهجمات إلكترونية. وفقًا لذلك فإن أي هجوم يتم على أوروبا أو أمريكا الشمالية يعتبر هجومًا ضد الجميع[٨٢].

(٨١) Misha Glenny, "The cyber arms race is on, as nations large and small mobilize to protect themselves and their enemies if provokd", **Pittsburgh Post-Gazette**, http://www.post-gazette.com/pg/11296/1183849-109-0.stm#ixzz1oMTYghXF

(٨٢) عبد الصادق، «القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني»: ١٣.

**خاتمة**

مما سبق نصل إلى نتيجة مفادها أن أشكال القوة تتغير بتغير التكنولوجيا، وقد أثر الفضاء الإلكتروني في الأشكال التقليدية للقوة، وطرح مفهومًا وشكلًا جديدًا هو القوة الإلكترونية. وقد كان لهذا الشكل الجديد دور في بلورة مفهوم انتشار القوة، وتعدد الفاعلين الممارسين لها، سواء من الدول أو من غير الدول، مما هدد الدور التقليدي للدول وقلل من سيادتها على إقليمها، ولم ينته الأمر عند ذلك؛ حيث ظهرت أشكال جديدة من الأسلحة. فعلى الرغم من ضآلة حجمها الذي لا يتعدى كيلو بايتس، وقلة تكلفتها، فقد تُسبب خسائر فادحة على مختلف المستويات الاقتصادية والسياسية والعسكرية، بل على المستويين الشخصي والفردي، فالضحية في هذه الحالة كل مشترك في خدمة الإنترنت، فالخسائر لا تعترف بالنوع ولا العمر ولا الإقليم. ومن ثم فمن الضروري وضع أطر حاكمة لاستخدامات هذه القوة وتقنينها بما يعمل على تحقيق الأمن الشخصي للمواطن، والأمن الدولي لمختلف الفواعل الدولية.




وحدة الدراسات المستقبلية
للاستعلام
تليفون: ٤٨٣٩٩٩٩ (٢٠٣) +؛ داخلي: ٥١٣٢
فاكس: ٤٨٧٩٢٥٢ (٢٠٣) +
الموقع الإلكتروني: www.bibalex.org



ISBN: 978-977-452-283-5